Enhancing Financial Inclusion through Digital ID

PROJECT DIRECTOR
Daniel F. Runde

AUTHORS
Romina Bandura
Sundar R. Ramanujam

A Report of the CSIS Project on Prosperity and Development

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
Enhancing Financial Inclusion through Digital ID

PROJECT DIRECTOR
Daniel F. Runde

AUTHORS
Romina Bandura
Sundar R. Ramanujam

A Report of the CSIS Project on Prosperity and Development

CSIS CENTER FOR STRATEGIC & INTERNATIONAL STUDIES
About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world’s greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS’s purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS’s values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies. All rights reserved.
Acknowledgments

The authors would like to express their deepest gratitude to several organizations and individuals whose contributions were indispensable in the production of this report.

The authors sincerely appreciate the February 2021 CSIS virtual roundtable attendees on digital ID, where participants and subject-matter experts shared their expertise and valuable insights. These attendees represented a diverse set of stakeholders in the development, security, and digital governance community and helped the authors enhance their research framework that yielded this publication. Several of these roundtable participants offered broad and unique expertise and provided constructive and substantive feedback as this report developed, and the authors are grateful for that. Special thanks to Hiromitsu Higashi and Elena Méndez Leal for their research inputs and support.

The authors would like to specifically thank Deon Woods Bell, Jeremiah Grossman, and Rebecca Weber at the Bill and Melinda Gates Foundation. This report would not have been possible without their constant guidance and the generous financial support from the foundation. CSIS is grateful for their trust with such a significant undertaking.
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Digital ID Systems as Enablers of Financial Inclusion</td>
<td>7</td>
</tr>
<tr>
<td>Designing Inclusive and Secure Digital ID Systems</td>
<td>9</td>
</tr>
<tr>
<td>Challenges in Implementing a Digital ID System</td>
<td>16</td>
</tr>
<tr>
<td>The United States' Role in the Digital ID Space</td>
<td>20</td>
</tr>
<tr>
<td>Conclusion</td>
<td>25</td>
</tr>
<tr>
<td>About the Authors</td>
<td>27</td>
</tr>
<tr>
<td>Annex 1: Definitions</td>
<td>29</td>
</tr>
<tr>
<td>Annex 2: Case Studies of Digital ID Systems: Estonia and India</td>
<td>30</td>
</tr>
</tbody>
</table>
Executive Summary

Although modern economies rely on citizens possessing a legal identity document (ID), more than 1.1 billion people remain without one. Countries have committed to fill this gap by implementing or expanding ID systems, with many attempting to leapfrog using digital ID systems. In simple terms, a digital ID is an innovative field that uses technology to assert and prove identity. They have the potential to streamline interactions among governments, individuals, and the private sector, creating economic efficiencies and lowering transaction costs. At the same time, digital IDs can also help advance financial, social, and political inclusion. At a fundamental level, a digital ID infrastructure that is properly designed and implemented could strengthen financial inclusion and integrity by reducing informal and illegal transactions and ensuring the ability to identify individuals and trace payments.

As with any new technology, digital ID systems also have risks and vulnerabilities. By instituting robust frameworks and controls and incorporating technology-based safeguards, digital ID systems can be insulated from exploitation by bad actors and government misuse, privacy and cybersecurity breaches, and system failures. With China increasing its footprint in the digital space, there are ample concerns that developing countries may swerve to a more authoritarian approach, with digital ID technologies being used to infringe on individual liberties as well as national sovereignty through espionage and data breaches. There is a real concern that these digital tools could also be used to effectively persecute ethnic minorities and other vulnerable groups in an environment devoid of
principles. Appropriate governance and accountability measures can also be ordained to ensure that the system remains reliable, secure, and inclusive. In sum, ID systems should be inclusive, protect privacy, and safeguard their integrity in order to build trust with users and maximize enrollment and growth capacity.

Implementing inclusive digital ID systems is a significant endeavor, requiring countries to invest in technological upgrades and carry out regulatory reforms. The United States has a significant opportunity—and a responsibility—to help mitigate risks and work toward better global digital ID infrastructure through its bilateral development agencies and the multilateral system. The United States funds and supports many important international programs related to digital ID systems, deploying development finance resources and sharing its technical assistance capabilities through its network of bilateral agencies. As the flagship development institution of the United States, the U.S. Agency for International Development (USAID) launched its Digital Strategy 2020–2024 to support open, secure, and inclusive digital ecosystems abroad. This is in addition to the efforts of the Millennium Challenge Corporation (MCC), the United States International Development Finance Corporation (DFC), and the Departments of Commerce, Energy, State, and Treasury.

While the United States does not currently have a national (or a digital) ID system that can serve as a blueprint for other countries, it still has an important role in this space as it advances its own interests. Specifically, the United States must catalyze global investments in hard infrastructure and other resources that can enable innovative technologies overseas. It must also draw upon its institutions (such as the National Institute of Standards and Technology, or NIST) to actively participate in global standard-setting bodies and ensure the integrity and interoperability of digital ID models. To that end, the United States government can build upon international and bilateral initiatives to support inclusive digital ID platforms in developing countries, focusing on the following five areas:

1. Finance investments in IT connectivity and workforce training
2. Invest in foundational ID systems and encourage a stack model for digital ID
3. Engage with donor and civil society partners to ensure that ID systems have appropriate data protections
4. Build international consensus around a framework that protects financial integrity
5. Increase USAID’s digital budget to help achieve ID for all

The United States needs to be more active in the digital ID space to ensure that the underpinnings of ID systems remain democratic and are not used as a tool of repression and surveillance. The United States must not take for granted that the advances in technology and digitization will automatically reinforce (and not weaken) democratic institutions. As governments seek to adopt innovative technology, the United States can partner with them to thwart any malicious use of these new technologies. Avoiding the misuse of these systems and abuse of data should be a fundamental priority as USAID and related development agencies work with countries and other donors.
Introduction

Around the world, 7.8 billion people engage in daily routines such as attending school, going to work, buying goods and services, traveling, and paying taxes. But to perform some of these activities, service providers often require a valid identity document (ID) in the form of a national ID, birth certificate, passport, driving license, or other form of official ID. Proof of one’s identity has become integral for both the public and private sector to allocate resources efficiently, allowing governments to deliver essential services to their citizens and to collect taxes. The private sector and small businesses also depend on official IDs to hire employees and conduct transactions. Specifically, under know-your-customer/anti-money-laundering (KYC/AML) standards, financial institutions need to verify a client’s identity to disburse a loan or send remittances; not holding a proper ID therefore acts as a deterrent to financial inclusion. In sum, many public and private services hinge upon the ability to identify people uniquely. As a result, the ability to “prove who you are” has become one of the most important foundations for people’s livelihoods.

Contemporary ID systems emerged in Europe around the period of the Second World War, with countries like the United Kingdom and France issuing physical (usually paper) documents to citizens through a national or state civil registry. In many of these advanced economies, IDs were created in an ad hoc way to enable governments to carry out specific functions such as collecting taxes, tracking welfare recipients, and distributing public healthcare benefits. This is evident in the history of U.S. Social Security Number, British National Insurance Number, and Canadian Social Insurance Number.
Since the end of the war in 1945, ID systems have mushroomed worldwide, although with differing characteristics (Box 1).

**Box 1: Types of ID Systems**

ID systems can be categorized either as foundational or functional. Foundational ID systems are those that are provided through civil registers, national IDs, and population registers, and which are to be used by citizens for a wide variety of transactions. On the other hand, countries can also have functional ID systems, which have a specific use for certain sectors (health, social security) or certain activities (voting, travel).

Historically, Britain and many of its former colonies like Canada and the United States did not develop a national ID or foundational ID system. These countries typically rely on specific functional credentials that are used as proof of identity—for example, social security numbers and driver’s licenses in the United States. In 2006, the United Kingdom attempted to institute a compulsory national ID for its citizens by enacting the Identity Cards Act, but this measure was widely unpopular.


For many people, the basis for legal identification begins at birth, with the registration of the newborn’s basic features (e.g., name, sex, place and date of birth) in an official civil registry. However, of the 140 million babies born every year around the world, 40 million will not have their birth registered. The lack of a legal ID system in several countries has left many people “invisible” to authorities and excluded from the modern economy. As of 2018, there are 1 billion people globally without a legal ID, mainly in developing countries (Figure 1). A McKinsey study finds that another 3.4 billion have an ID but cannot authenticate it digitally. Women are especially disadvantaged in this regard, with one out of two of women living in low-income countries (LICs) lacking access to a legal ID. To fill this gap, countries around the world have committed to expanding IDs to their citizens. The United Nations’ Sustainable Development Goal (SDG) 16, target 16.9, calls on countries to “provide legal identity for all, including birth registration” by 2030. A related goal, 17.19, urges countries to increase their data collection capacity by monitoring the “proportion of countries [that] have achieved 100 per cent birth registration and 80 per cent death registration.” This ambitious goal will not come cheaply; the World Bank has estimated a price tag of $9 billion to achieve identification for all.
With the advent of innovative technology, paper ID cards have evolved into digital credentials. Digital ID in its simplest form is “the use of technology in asserting and proving identity” (see Annex 1 for definitions).\(^{19}\) According to the most recent World Bank ID4D dataset, 175 countries currently have a national ID database, while 161 are supported by digital technologies.\(^ {20}\) Digital ID systems exist in various forms in Canada, the United Kingdom, Finland, Sweden, Estonia, Nigeria, Singapore, Thailand, India, and Argentina. India (with its Aadhaar system) and Estonia (with its e-ID) represent countries with the highest adoption rates among the population, with take-up above 90 percent (see Annex 2). Other countries have a mixed record in launching their digital ID systems, but many are now exploring the idea, given the advantages of digital IDs over their paper-based counterparts.

Digital IDs have the potential to streamline interactions among governments, individuals, and the private sector, thus creating economic efficiencies and lowering transaction costs.\(^ {21}\) At the same time, digital IDs can also help advance financial, social, and political inclusion. Digital IDs can be a particularly important enabler of financial inclusion by simplifying customer due diligence (CDD) and authentication processes, thereby allowing for the transfer of secure payments. For governments, digital IDs can improve their capacity to deliver essential public services to underserved populations. In the current global pandemic context, for instance, without any way to identify those in need of Covid-19 vaccination, countries can potentially miss vulnerable populations, creating weak links in their public health systems.\(^ {22}\) In addition, the use of digital IDs allows for greater government accountability, as it creates a reservoir of data and metrics that the state can subsequently use to assess the impact of its programs.

The adoption of digital ID systems does come with its own risks. Without proper frameworks and controls, they are vulnerable to exploitation by bad actors and government misuse, privacy and
cybersecurity breaches, system failures, and the possible exclusion of individuals. Although these risks also apply to traditional paper-based ID systems, breaches can be more devastating in a digital environment due to the potential scale of the attacks.²³ Thus, appropriate technology-based safeguards, along with governance and accountability measures, are needed to address and mitigate these risks. Moreover, with China increasing its footprint in the digital space, there are ample concerns that developing countries may swerve to a more authoritarian approach, with such technologies being used to infringe on individual liberties as well as national sovereignty through espionage and data breaches. There is a real concern that in an environment devoid of principles, these digital tools could also be used to effectively persecute ethnic minorities and other vulnerable groups.²⁴ History has painful examples of these trends, such as the Kennkarte ID system which was used to persecute the Jewish community in Nazi Germany.²⁵

Implementing inclusive digital ID systems is a significant endeavor, requiring countries to invest in technological upgrades and implement regulatory reforms. With many countries looking to upgrade their ID systems, it is important that resources be well spent. As countries develop digital ID systems, the United States has a significant opportunity and a responsibility to help mitigate risks and work toward better digital ID infrastructure around the world through its bilateral development agencies and the multilateral system.²⁶

Although the United States does not currently have a national ID system (nor a digital ID system) that can serve as a blueprint for other countries, it can still play an important role in this space. The United States can also advance its own interests as regards development, security, and commerce by investing in hard infrastructure and enabling innovative technologies abroad, by setting standards (such as through the NIST), by actively participating in global standard-setting bodies, and by ensuring the integrity and interoperability of digital ID models.²⁷ Specifically, assisting countries in the design and implementation of sound digital ID systems can be instrumental in enhancing financial inclusion.
A lack of proper ID acts as a significant deterrent for financial inclusion—especially for vulnerable groups, including the poor, rural communities, women, and refugees, who oftentimes do not possess any type of legal documents or only have some of poor quality.\textsuperscript{28} An ID is often required to contract different financial services, from opening an account to customer onboarding, making payments, getting a loan, and others. According to data by the World Bank, 90 percent of commercial banks require a government-issued ID to open a deposit account.\textsuperscript{29} Moreover, countries are increasingly requiring an official ID to purchase a mobile phone, get a SIM card, or open a mobile money account.

Many people thus resort to unregulated and informal channels to conduct financial transactions. This practice lends itself to a series of risks for the individual (such as high transaction costs, risk of exploitation, identity theft, and fraud) and for the institutions and overall financial system (such as cyberattacks, money laundering, and terrorism finance). Thus, designing an inclusive digital ID can be a crucial first step in increasing financial inclusion (Box 2).\textsuperscript{30}
Box 2: Digital ID and Financial Inclusion

Digital ID has the potential to increase financial inclusion by

a. Allowing people to open an account by simplifying documentation requirements,

b. Enabling customers to onboard remotely and inexpensively, and

c. Supporting the delivery of additional financial services through digital signatures and obtaining customer consent.


According to the intergovernmental organization Financial Action Task Force (FATF), one main challenge that financial service providers face when trying to bring people into the formal and regulated financial sector is identifying the customers and then verifying their identity. Financial sector regulations require financial service providers (banks, insurance companies, and others) to verify who their customers are, in order to ensure that the funds involved are not linked with illicit activities such as money laundering, crime, and terrorism. Institutions apply regulations such as appropriate CDD to ensure the security of transactions and overall data integrity of the financial system. At the same time, applying an over-restrictive approach to illicit finance safeguards can also exclude legitimate prospective customers from the formal financial sector. Thus, a balance needs to be struck when designing regulations to ensure that financial inclusion and financial integrity become mutually reinforcing.

In order to comply with illicit finance regulations while also enabling financial inclusion, regulated institutions apply a “tiered CDD.” This means that the level of access that a person gets to a range of account functionalities and financial services depends on the identification or verification conducted by the regulated entity. So, for example, access to basic account services (like depositing small sums of money) requires minimum identification, while access to more complex services and higher monetary values is only allowed if the customer provides the required additional ID verification information.
Designing Inclusive and Secure Digital ID Systems

In the context of financial services, a digital ID allows financial institutions to simplify their CDD processes without compromising on the safety and integrity of the transactions. For example, a digital ID can enable the customer verification process to be done remotely or at an agent location, removing the need for maintaining paper records. Further, digital IDs can be effective in fintech models like open banking (the practice of sharing financial information electronically, securely, and only under conditions that customers approve of), since these models rely on strong customer authentication to access data and accounts.

Innovative technologies can enable more streamlined ID systems while protecting the privacy of the user and the integrity of the system. Digital ID systems may use technologies such as biometrics, mobile devices, smart chips, SIM cards, barcodes, PINs, and blockchain technologies (see Figure 3). However, not all elements of a digital ID system are necessarily digital: some elements can be either digital or physical (e.g., paper, plastic, or others), or a combination of both.
Figure 2: Identity Lifecycle


Figure 3: Technologies Used in the Digital ID Cycle

Nevertheless, there is no “one size fits all” design for digital IDs that can be replicated across countries. Specific digital ID systems vary in approach, level of digital integration, trust and transparency, and adoption. As the FATF asserts, there currently are no comprehensive internationally agreed standards for developing digital ID systems; there exists instead a range of global standards at each point of the ID lifecycle. However, numerous global initiatives have laid out certain principles to guide in the design of digital ID systems. The Principles on Identification for Sustainable Development (ID4D), endorsed by 30 international organizations such as the World Bank and UN agencies, along with FATF’s Guidance on Digital Identity, offer guidance on how development actors should think about designing a digital ID. Proposed principles can be captured by the following three categories (Figure 4):

**Figure 4: Main Principles of ID Systems**

![Figure 4: Main Principles of ID Systems](image)

**Inclusion:** If the goal of an ID system is to provide documentation to an entire population, the ID should not be tied to any other attributes used to discriminate against (or harass) individuals. This feature of nondiscrimination should be codified in statutes and policy and practiced by developing inclusive communications strategies, enrollment systems, and data protection efforts. The success of an ID system also depends on how easy it is for people to access it. Therefore, fees associated to the service should not be prohibitive and no one should be denied an ID because they lack digital skills or digital devices. For example, in the case of the Aadhaar ID card, Indian citizens do not have to pay any fees or incur any monetary costs to obtain their ID when they enroll for first time, which makes it accessible to everyone. It is also critical that the system has an intuitive design, meaning that a regular person can figure out how to use it.

**Sustainability:** ID systems should not be developed in a vacuum without any concern for their feasibility and their usefulness. Therefore, a digital ID system should be financially and operationally sustainable in the long run. It must respond to the changing needs and challenges of the population that lacks proper documentation. One important aspect is the interoperability of an ID system. That is, the ID system should be integrated and accepted across entities and services: it should work across
different levels of the national government, between the national and sub-national government, in regulated commercial and retail establishments, and (potentially) by foreign governments. In order to foster innovation, the software and specifications underlying ID systems should be developed using open standards and maintained by a community that shares data across tools and systems (for example through the Modular Open Source Identity Platform, MOSIP). Doing this lowers the unit cost for the private sector and spurs innovation without locking in a vendor or favoring select firms. Estonia is a quintessential example of how robust regulatory frameworks coupled with public-private partnerships can maximize the durability, impact, and sustainability of a digital ID system, with the Estonian government making it easier for the private sector to innovate using its IT infrastructure and thus keeping the system up to date and relevant to the evolving needs of the society. Other examples include the Indonesian national digital ID (the electronic Kartu Tanda Penduduk, or e-KTP) that was launched nationwide in 2011 and quickly became integral to participating in socioeconomic and civic life, including voting and other commercial CDD efforts. By 2019, over 98 percent of the population were enrolled.

**Privacy and Integrity:** Financial transactions carry certain risks. There are risks to the individuals (e.g., customers’ accounts may be hacked or spoofed) and risks to the system (e.g., in the form of money laundering and terrorism financing). Building trust in the system is vital to ensure that the population fully accepts the identification document and uses it. Bad actors (such as terrorists and criminals) may be able to abuse digital ID systems by either creating false identities or exploiting legitimate people. In 2016, the Philippines Commission on the Elections acknowledged that the records of more than 70 million electors (including fingerprint data and passport information) were compromised because of a data breach that occurred ahead of their general elections. The breach exposed the database system’s vulnerabilities and lack of robust defenses against cyberattacks. Similarly, India’s Aadhaar database (that carries the sensitive information of over a billion people) lacked a meaningful data protection and cyber defense system, which led to its database being plundered in 2018, allowing malicious actors to steal identities for as little as $7. Considering the gravity of these recent events, it is imperative that foundational ID systems are created with sufficient robustness checks, so that the data collected from the individual remains unique, secure, and accurate. Once the identity data is collected, this highly sensitive information should be safeguarded by investments in cybersecurity infrastructure as well as a strong legal framework that prioritizes people’s rights and privacy. Both the managers and the regulators of the ID systems should clearly outline responsibilities and be subject to oversight and accountability. If any of these safeguards develop glitches, there should be a procedure for redress, including recourse to independent judicial adjudication. The government should ensure that such provisions are enacted by law. In that regard, the Estonian model can be showcased for its strong legal and institutional framework (coupled with an information and communications technology [ICT] system with privacy-by-design features) that generates a high level of trust among the public in national e-governance. Similarly, the decentralized identity authentication system in Austria uses tokenization technology to protect its citizens’ privacy, while citizens can access an audit trail to monitor the use of their data.

ID systems and customer verification are also important to safeguard the integrity of the system against financial crimes. Thus, countries need to develop digital ID assurance frameworks and standards to assess risks to the financial system and mitigate these risks. A risk-based approach (RBA) needs to be applied to determine the extent of the CDD process: greater measures are required in situations that imply a higher risk of money laundering or terrorism financing, while simpler
measures may be appropriate in situations where low risk is established. In sum, regulated financial providers need to apply CDD measures that are commensurate with the type and level of the risk of illicit finance.

Taken together, ID systems should be inclusive, protect privacy, and safeguard the systems’ integrity in order to build trust with users and maximize enrollment and growth capacity. A recent McKinsey study emphasizes that a successful digital ID scheme is one that is able to cover a large proportion of the population and bring together both private and public sector providers. Implementing a digital ID has many challenges, but countries can take six steps in this process: design the right model, make the system interoperable with other systems (such as financial sector and healthcare providers), ensure wide coverage, guarantee that the system can be used for different purposes, design it so that it is easy and convenient to use, and make sure that the privacy of people’s information is protected to establish a foundation of trust in the system (see Box 3).

Box 3: Six Steps for a Successful Digital ID System

1. **Adopt a Specific Operating Model:** The first step in implementing an ID system is choosing which entity will be responsible for operating the system, meaning what trusted source will enroll users, authenticate users, issue the ID credentials, and integrate other service providers. The choice is between a “centralized” model (i.e., a single government entity takes on these functions), a “federated” model (i.e., several entities, including private companies, are involved in the digital ID system) or an “open market” (i.e., different providers enter into bilateral agreements with individual government agencies). The selection between these models will depend on factors such as the reliability and efficiency of existing digital ID infrastructure, public attitudes toward (and trust in) the private sector, and the likelihood of the model encouraging rapid enrollment.

2. **Ensure Interoperability:** A second important feature is that different systems need to be integrated or interoperable, that is, they need talk to each other so that the single ID is accepted across platforms—for example, so that the ID can be used to access healthcare databases as well as government services. Interoperability allows a digital ID to be most useful across multiple jurisdictions as well as in the private sector. It also stops the proliferation of IDs, which could lead to fragmentation. Committing to best practices from successful digital ID models around the world and leveraging new technologies that enable a seamless transfer of data between systems can help achieve interoperability.

3. **Put in Place a Regulatory Framework That Expands Usability:** Regulations should allow the ID to be usable across both the private and public sectors and make it easy to complete verification and authentication processes using a range of digital indicators. The private sector has a significant role to play in making the digital ID ecosystem widely and universally accepted—once the public sector invests in the foundation framework.

4. **Link to Other Services:** To ensure that IDs are valued and useful to the user, governments should link digital ID systems with every public-sector service delivery if possible, while creating channels and avenues for greater adoption of the ID in the retail and commercial space.
5. **Design It to Be Customer Friendly:** Much like other commercial activities, a move toward digital IDs should not create an added burden on the user. To that end, users should find the system accessible, affordable, convenient, fast, intuitive, and straightforward. A positive user experience helps meet the user’s expectations of the process, which goes a long way in boosting its acceptance and adoption by the public.

6. **Build User Trust:** The design and development of the ID system must be centered around the user’s privacy. Successful models should consider how data collection and storage can be done safely and effectively while ensuring fundamental protections of privacy and data security.


With new technologies emerging, governments are pursuing digital transformation within their services. Following the lead of countries such as Estonia, Singapore, and India, there is growing interest in how governments can reach citizens through a base level of infrastructure upon which third-party vendors can build new applications and services. This “GovStack” approach allows essential services to sit on top of base layers, the “stack” of essential components like digital ID, finance, and data. Software engineers use “stacks” to design independent platforms that serve specific functions, and countries can similarly use a stack model to realize digital transformation. This layering of services (reminiscent of a layered cake, see Figure 5) in a “digital government stack” framework identifies three tiers of digital protocols (digital identity, data exchange, and digital payments) that underlie other digital government applications (such as public registries, land titling, taxation, procurement, benefits management, and civic participation) and facilitate government service provision. Regardless of the type or model, countries can conceive of their digital ecosystem as the following sequence of stacks:

1. **Base:** Securing critical infrastructure such as connectivity, power, and workforce capacity (e.g., engineering and digital skills). Digital capacity and literacy of citizens is also an important component.

2. **Foundational Layers:**
   - A trusted and inclusive digital ID system (foundational ID)
   - A fully developed database management system that can be accessed securely, as an ecosystem or federation of data sources that are interoperable and can exchange data as needed
   - A digital payment interface that is integrated with the public sector for taxation and welfare distribution

3. **Application or Use Case Layers:** Once the above stacks are developed through public-sector investments, the government can open up the digital ecosystem to cross-sectorial applications and other innovative services, while remaining the authoritative source of identity.

4. **Toppings:** Once the core government infrastructure is in place, new apps and services that are built locally by national innovators can be placed on top.
With such a layered approach, the deployment of these advanced digital IDs means that, in practice, one digital ID can provide many functions to the holder, from receiving healthcare to voting to driving. For example, Estonia’s digital ID follows this digital stack approach and is at the vanguard of the EU digital ID movement. In 2019, the European Union passed legislation to require the rest of its member states to implement changes to the technology and security features of ID cards to bring them up to the same level as passports over a two-year period, allowing citizens to carry several functions using a single ID. A separate EU regulation on electronic identification and trust services for online transactions called eIDAS (electronic Identification, Authentication and trust Services) was passed in 2014.53

Figure 5: Building Blocks of the “Digital Government Stack”

Source: Reprinted with permission from Kate Wilson, Digital Impact Alliance.
Challenges in Implementing a Digital ID System

Applying these guiding frameworks and principles onto a country context is not an easy feat: there are governance, institutional, and logistical considerations to implementing a successful digital ID system. Digital IDs involve financing investments in hard infrastructure as well as creating the regulatory and legal frameworks governing these systems’ use to guard them against cyber intrusions. Rolling out all these elements costs money, with the World Bank’s ID4D determining that the cost of implementing a foundational ID system depends on multiple factors.54

Core Cost Components: These are responsible for 90 percent of the total implementation costs, and they include human resources development, infrastructure procurement, investment in information, education, and communication campaigns.
**Country Characteristics:** These include high-impact characteristics (population, wage levels, telecom density, and urban-rural density) and medium-impact characteristics (topography, skilled labor density, literacy levels, and reliable energy infrastructure).

**Program Design Choices:** These are design choices that impact the costs of implementation and vary according to the policy preferences of individual governments establishing the ID system. They include credential medium choices (which can vary from being 3 to 40 percent of the overall costs), choice of biometrics, enrollment timelines, integrated administration of civil registration and identification, and number of biographic fields.

Given how unique and adaptable to each country a foundational ID system needs to be, estimating implementation costs remains a challenging exercise. One estimate finds that the average investment of enrollment and credentialing can average between $4 and $12 USD per person. That said, countries with large populations can use economy of scale and bring the overall costs down, such as India, which achieved a $1.16 per person cost for its Aadhaar card. The lack of a smart card requirement also kept the costs low, indicating the impact that the choice of credential has on costs. Many developing countries lack the financial resources to invest in infrastructure, while their national and local governments have weak capacity to design ID systems and operationalize them. Furthermore, coordination and partnerships with the private sector are also important elements. Finally, there are equity considerations that need to be factored in, since women,
minorities, migrants, and other historically disadvantaged groups are often at greater risk of societal exclusion, furthering the digital divide.

Creating a functional digital ID system requires a certain degree of “hard” physical infrastructure to work, including round-the-clock electricity access, high-speed internet connectivity, increased mobile network penetration, and low-cost access to biometric technologies, smartphones, and other digital tools. However, many countries start developing digital IDs well before this ideal is achieved. Digital infrastructure requires investments in energy, telecommunications, and utility sectors. In part, this challenge needs to be met by investments in expanding the coverage of high-speed mobile networks to over 85 percent of the global population, who need it for faster transactions at points-of-sale; even more fundamentally, it requires securing electricity access to unpowered communities, catering to about a billion people globally. These prerequisites need to be addressed before establishing thousands of IT-powered ID enrollment centers and associated data storage centers. According to estimates from the Global Infrastructure Outlook, given the current trends, an additional $4.2 trillion in global infrastructure investment will be needed by 2040 to meet the demand.

According to a McKinsey study, digital ID systems not only rely on basic infrastructure, such as internet and power, but also on specific components and capabilities such as the IT infrastructure used for “enrollment, back-end data processing, and authentication, as well as the physical features needed for user interaction and registration.” In the financial services sector, for example, verifying the identity of clients using biometric data (e.g., fingerprints and iris scans) requires adequate readers, energy, and internet connectivity to allow for real-time authentication. Moreover, institutions need to make sure that their network of agents is also equipped and capable to conduct identity verification, as well as to guarantee that the risk of identity fraud is adequately managed. In sum, the IT requirements, training, capacity, and costs of using a real-time verification system can be significant for financial institutions.

There are also “soft infrastructure” requirements that governments need to keep in mind when establishing digital IDs, such as the evolving global norms and workforce skills surrounding emerging technologies and digitization. Countries need legal frameworks and global standards to guide the implementation of ID systems. Strong legal, regulatory, and operational frameworks should ensure that ID systems minimize risks and are implemented effectively, and that standards are set around issues such as data collection privacy. The rules and frameworks governing digital IDs can increase community benefits and individual access to government services, but they can also be used as an authoritative tool to infringe on individual rights and freedoms. If appropriately implemented, digital ID systems that prioritize personal freedom and access offer the potential to mitigate the risk of fraud and data mismanagement and create a lasting framework that can improve how individuals, societies, and the world interact as technology changes. In the financial sector, the FATF recommends that data protection and privacy measures be implemented across the system to ensure data integrity, so as to prevent data leakages that can facilitate identity fraud (including by money launderers and terrorist financiers), to protect individuals’ privacy, and to combat abuse.

Implementing digital ID systems also requires cooperation and coordination from various stakeholders, including governments, civil society, and the private sector. This coordination includes developing interoperable systems and investing in infrastructure and technology. The joint work of government and nongovernment institutions to digitize databases, credentials, and other forms of data transfers will be critical to any digital ID system’s success.
Finally, implementing digital ID systems must carry inclusion and equity considerations. Vulnerable and excluded groups have added challenges related to technology (such as lack of IT access) and are more likely to be subject to violence, harassment, or exploitation should their data become public. Similarly, the adoption of digitization can exacerbate existing gaps, for example in places where social norms foster greater adoption by men than women. On the other hand, in the case of migrant groups, digital IDs can facilitate their access to needed social services and humanitarian assistance (see Box 5).

**Box 5: Digital ID and Migration**

Digital IDs can enable societal inclusion for migrants. Globally, over 1 billion migrants (of which more than 7 percent are refugees and asylum seekers) face challenges in securing admission when transit and host countries enforce border management policies through identity checks and passport verification. The unplanned nature of displaced populations’ movements makes it difficult for them to provide legal documentation that can determine their identity. In refugee camps, for example, the World Food Program is rolling out blockchain technology, though its “Building Blocks” pilot, so Syrian refugees can access cash assistance.

Even if admitted into a country, the lack of an ID poses medium- and long-term economic access and equity challenges as migrants struggle to restart their lives. They may be unable to join the financial system, secure a mobile connection, or fulfill most CDD requirements necessary for various retail and public sector services. In this context, digital ID can be a game changer and simplify the admission and settlement process for forcibly displaced migrants while assuring that border management agencies are able to keep track of displaced populations. However, an ethical framework governing digital identity for refugees and migrants should address concerns around migrants giving up personal data and information without their meaningful consent.
The United States’ Role in the Digital ID Space

A safe, robust, and resilient digital environment is a key imperative for U.S. interests in a global interconnected world. As CSIS has previously underscored, the burgeoning demand for digitization in the developing world has created a first-mover’s advantage in this market. The window of opportunity to lead the market is fast narrowing as the global race for technological dominance heats up between the United States and its geopolitical competitors. Development finance institutions can support some of these early investments to facilitate the entry of U.S. ventures in the developing world, fund infrastructure projects critical to launching digital ID systems, and grow indigenous markets whose products are consistent with the U.S. values of freedom, innovation, and opportunity.

A global digital ID market shaped early on by U.S. investments is more likely to have safeguards and checks built into the system to ensure data privacy; protection from cyberattacks, espionage, and surveillance; and resilience against external shocks. Absent U.S. leadership risks that authoritarian states will increasingly compete and gain dominance in the global cyber governance architecture, to the detriment of U.S. national security interests. As President Biden has laid out in the Executive Order on Improving the Nation’s Cybersecurity, the United States needs to strengthen its cybersecurity defenses at home and abroad so that the U.S. government and the private sector are more resilient to cyberattacks and other malicious incidents.
Recognizing these challenges, the push to develop digital ID systems has already been playing out in the international arena through the United Nations’ SDGs, World Bank’s ID4D, and other initiatives. The United States funds and supports many of these and other important international programs. It also deploys development finance resources and technical assistance capabilities through its network of bilateral agencies to help countries adopt digital solutions. USAID, as the premier development institution of the United States, has recently launched its Digital Strategy 2020–2024, which is aimed at supporting open, secure, and inclusive digital ecosystems abroad. This strategy is being implemented by the Technology Division within the Innovation, Technology and Research Hub of the Bureau of Democracy, Development and Innovation (DDI). In addition to USAID, other relevant U.S. agencies involved in this space include the MCC and the DFC, as well as the State, Commerce, Energy, and Treasury Departments.

Given these considerations, the U.S. government can build upon these initiatives to support inclusive digital ID platforms in developing countries, focusing on the following five areas:

1. **FINANCE INVESTMENTS IN IT CONNECTIVITY AND WORKFORCE TRAINING**

For digital ID systems to work, developing countries need to have their basic digital infrastructure foundation in place, such as reliable energy, internet connectivity, and mobile technology. This amounts to billions of dollars in financing which must be mobilized through domestic resources, foreign aid, or private capital. Although the U.S. government has not traditionally funded physical infrastructure directly as part of its development architecture (aside from investments in Iraq and Afghanistan), there are agencies that support the software and environment to enable digital infrastructure. USAID and MCC have been providing significant technical assistance through initiatives such as Power Africa, the new Digital Ecosystem Fund (DEF), and MCC country compacts and threshold programs. With the DFC ramping up operations in low-income and lower-middle-income countries, this agency has a chance to mobilize significant private capital for infrastructure, especially as it relates to ICT and digital services. In its 2020–2025 strategic plan, the DFC has committed $5 billion in “Open, Interoperable, Reliable and Secure Digital Infrastructure and Internet Access.” Within this vision, DFC aims to increase internet access for 3 million people. At the same time, it has committed to $10 billion in energy sector investments with the aim to increase electricity access for at least 10 million people by 2025.

That said, there is also vast human capital that needs to accompany the development of this critical infrastructure. More resources are needed to educate and train the workforce for 4IR technologies and ICT-related fields. This includes professionals such as engineers, IT administrators, data operators and managers, along with other vocational trades like electricians. Additionally, governments will also need to enhance their law enforcement and justice system capacities by training and hiring more lawyers, judges, police officers, and other administrative staff. To support countries in this endeavor, USAID could increase its technical assistance for workforce development. As CSIS argued in a 2018 future of work report, some ways to enhance the capacity of USAID in skills development and employment could include creating an “Employment and Workforce Office” staffed with qualified labor expertise. This could be a way to offer more technical assistance to developing countries on employment and workforce issues. USAID could shift budgets from other departments to fund this new office. Moreover, to increase coordination, collaboration, and development impact, this new office would need to interact regularly with other related USAID offices, such as Education and Economic Growth, to avoid a siloed approach to these issues. At the same time, USAID could strengthen its links...
with the World Bank and International Labor Organization (ILO), both at the global and the country level, to equip workers with digital skills.

2. INVEST IN FOUNDATIONAL ID SYSTEMS AND ENCOURAGE A STACK MODEL FOR DIGITAL ID

Besides issues of connectivity and workforce training, the U.S. government should work with other development actors, such as the World Bank's ID4D initiative, in helping countries build foundational ID systems. When designing digital ID systems, USAID can encourage countries to build an interface that starts with the identification database as its foundational layer, upon which other functions or layers can be added. ID does not exist in a vacuum; it is a part of the broader digital stack of payments, data, and interoperability. Countries and donors therefore need to be thinking about ID systems for service delivery, particularly in the digital domain. By developing this ID layer, governments can define data use terms, thus keeping the digital ID universal, interoperable, and secure. This also allows governments to establish the regulatory sandbox within which private-sector partners can innovate and build out new application layers. What is important is that the ID can link to the original database layer and provide a host of other public and commercial services—such as voting, receiving subsidies, utility registration, employment benefits, and more.

As the ongoing fourth industrial revolution leads to a proliferation of new technologies, multiple competing ID systems have already been put in place. This could lead to the multiplication of new digital ID programs that are defined by the technology itself and constrained to a narrow set of issues. An identification document born from a public service delivery system—like social security or taxation—can be inefficient and can lead to a proliferation of IDs that may not always be universally accepted. In contrast, designing cross-cutting ID systems requires a long-term view, which creates the opportunity for developers to use open-source platforms and standards with interoperability at their heart. Having interoperable ID systems that can link other national services together can improve access and service delivery for citizens across a variety of sectors, including health, education, social welfare, and financial inclusion.74

The most notable example is the India Stack, the world’s largest application programming interface (API), which caters to the e-governance needs of over a billion users.75 The origins of the India Stack can be traced to the establishment of the Aadhaar identification document in 2009, which created the stack’s first layer in the form of a database of biometric information used to verify an individual’s identity. In 2011, the India Stack evolved to add a public service delivery layer, making it easier for the government to use the foundational database and target the beneficiaries of welfare subsidies. As more layers were added over time, both public and private sector actors have been able to use the India Stack to facilitate digital payments, digitally store certified documents, and perform KYC checks at various points of sale. There are many important lessons to be learned from this and other ID systems that the United States can translate in other developing country contexts.

3. ENGAGE WITH DONOR AND CIVIL SOCIETY PARTNERS TO ENSURE THAT ID SYSTEMS HAVE APPROPRIATE DATA PROTECTIONS

As already argued, the hallmark of an inclusive ID system is its ability to protect access to sensitive and vital information. When governments seek to adopt new technologies, the primary challenge is to establish appropriate safeguards to ensure that any systems that hold sensitive information are not used by powerful entities for malicious purposes. Although digital IDs can be the next frontier, there
is a real risk that political leaders will use state power to discriminate against their own people or persecute vulnerable groups of society.

At the same time, there are legitimate concerns that the involvement of outside actors could further some of these repressive tendencies. China is actively supporting infrastructure development abroad, including digital technologies. In the digital space, through its Digital Silk Road initiative, China is providing financing to expand developing countries’ telecommunications networks, artificial intelligence capabilities, and e-commerce and mobile payment systems, among others. With China increasingly investing in the global digital economy, there is a real danger that it will export a more authoritarian approach to development—that is, provide technologies that can be used for social control, to infringe on personal freedoms and further authoritarian tendencies. This technology can also endanger country sovereignty through measures like espionage and data breaches, which could enable China to obtain data from other countries for its own authoritarian uses.

Through the State Department, the National Endowment for Democracy, and USAID, the United States can use its moral authority to ensure that digital ID systems do not make it easier for quasi-authoritarian actors in developing countries to harm the most vulnerable in their societies. As democracy promotion advocates have demonstrated, the key to inclusive governance models begins and ends with civil society engagement. A diverse coalition of civil society actors can help governments design privacy regulations, which can lead to de-risking privacy concerns around a centralized ID database while also incorporating breaks in the state’s ability to have unencumbered access to sensitive information. Civil society actors can also be a key element in monitoring and evaluating the robustness of such checks on state power, and together with legislative groups, they can compel government actors to observe the state’s commitment to protecting the privacy and civil liberties of vulnerable social groups.

4. BUILD INTERNATIONAL CONSENSUS AROUND A FRAMEWORK THAT PROTECTS FINANCIAL INTEGRITY

Further risks to ID systems stem from illicit finance, where the United States has a lead role in preventing the global financial system from becoming a more conducive platform for criminal activities. This can be realized in part by building consensus in multilateral bodies among natural allies and like-minded partners—like the G7, Five Eyes, and the Quad—to adopt digital ID principles that address the risks of increased financial crimes. Specifically, such principles would advance a digital ID system that would not only be inclusive but would also incorporate robust assurance frameworks that can enhance law enforcement agencies’ ability to pursue their AML and combating financing of terrorism (CFT) efforts. The resulting system should allow the possessor of a digital ID to undergo CDD with ease and without discrimination, and it should comply with financial anti-criminal enforcement institutions and protocols with ease.

The intergovernmental FATF, which has the mandate to develop policies that countries can use to pursue AML/CFT efforts, lays out its technology-agnostic guidance on how governments can consider the development of robust assurance frameworks. Building on this, U.S. agencies such as the Department of Treasury and the NIST (housed under the Department of Commerce) can lead the government’s interagency efforts, bringing together stakeholders of data privacy and financial integrity with relevant actors in the private sector to give to the world a set of technical standards that is both secure and robust in its assurance levels.
5. INCREASE USAID’S DIGITAL BUDGET TO HELP ACHIEVE ID FOR ALL

Finally, more resources from the U.S. government (in terms of money and staffing) should be devoted toward building inclusive ID systems abroad to achieve identification for all by 2030, with USAID leading the effort. As argued in this brief, digital IDs are a crucial component for human dignity and a powerful tool to advance social, political, and financial inclusion. Since digital development is a cross-cutting issue, investments and commitments in this area are spread out across federal agencies and sectors. This makes it difficult to paint a comprehensive picture on the investments the U.S. government should dedicate to supporting digital ecosystems abroad.

USAID’s digital programs relate to topics such as humanitarian assistance, democracy strengthening, and financial inclusion. Through its Technology Division at DDI, USAID has requested a budget of $82 million for FY 2021 to implement its Digital Strategy. However, the National Security Commission on Artificial Intelligence (NSCAI) has estimated that USAID will need a yearly budget of $200 million—and even multiples of that—to support country efforts and increased staffing. These resources could be allocated to increase USAID’s own Digital Ecosystem Fund and bolster international initiatives such as the World Bank’s ID4D, as well as to support open-source platforms such as MOSIP.
Conclusion

The ability to authenticate and verify the identity of an individual in the digital era will become increasingly relevant to achieving more inclusive societies, while at the same time representing an important safeguard to individual privacy and the integrity of systems.80 The number of global digital transactions is growing at an astonishing rate, at an average of 13 percent per year. Furthermore, estimates suggest that 60 percent of global GDP will be digitized by 2022. Given these trends, countries can leverage new technologies to develop inclusive digital ID systems that are designed with their citizens’ consent and which ensure citizens’ control over their own data.

Developing countries are increasingly coming under pressure to modernize and digitize their economies, and Covid-19 has only compounded this challenge. At a fundamental level, a digital ID infrastructure that is properly designed and implemented could strengthen financial inclusion and integrity by reducing informal and illegal transactions and ensuring the ability to identify individuals and trace payments. Specifically, investing in the design and implementation of sound digital ID systems can be instrumental in enhancing financial inclusion.

The United States needs to be more active in this space to ensure that the underpinnings of ID systems remain democratic and are not used as tools of repression and surveillance. The United States must not take for granted that advances in technology and digitization will reinforce rather than erode democracy.81 As governments seek to adopt innovative technology, the United States can work in
partnership with them to thwart these new technologies from being used for malicious purposes. As USAID and related development agencies work with countries and other donors, avoiding the misuse of these systems and abuse of data should be a fundamental priority.
About the Authors

Daniel F. Runde is senior vice president, director of the Project on Prosperity and Development (PPD), and holds the William A. Schreyer Chair in Global Analysis at the Center for Strategic and International Studies (CSIS). A global thought leader and change agent, his work centers on leveraging U.S. soft power and the central roles of the private sector and good governance in creating a more free and prosperous world. Mr. Runde has been recognized for influencing the debate on USAID-State Department relations, as an architect of the BUILD Act, and for leading the debate surrounding the role and future of the World Bank Group. Mr. Runde has also influenced thinking about U.S. economic engagement with Africa (of which he is in favor of much more) and domestic resource mobilization. Mr. Runde holds the Officer’s Cross in the Order of Isabel la Católica, a Spanish Civil Order.

Previously, Mr. Runde held senior leadership roles at the International Finance Corporation (IFC). From 2005 to 2007, he was director of the Office of Global Development Alliances (GDA) at USAID, and he led the GDA partnership initiative by providing training, networks, staff, funds, and advice to establish and strengthen public-private partnerships. His efforts at USAID leveraged $4.8 billion through 100 direct alliances and 300 others through training and technical assistance. Mr. Runde is the chairman of the Advisory Committee on Voluntary Foreign Aid (ACVFA), and he
also serves as the chair of the Sub-Saharan Africa Advisory Committee for the Export-Import Bank of the United States (Ex-Im). He also serves on the board of the International Foundation for Electoral Systems (IFES), the Millennium Challenge Corporation (MCC) Advisory Council, the Western NIS Enterprise Fund (WNISEF), and the Ashesi University Foundation (a private university located in Accra, Ghana). Mr. Runde is also a lifetime member of the Council on Foreign Relations (CFR) as well as a member of Bretton Woods. Mr. Runde is a regular contributor to The Hill and hosts a podcast series, Building the Future with Dan Runde: Freedom, Prosperity, & Foreign Policy.

About the Authors

Romina Bandura is a senior fellow with PPD and the Project on U.S. Leadership in Development at CSIS. Her current research focuses on the future of work in developing countries and the United States’ economic engagement in the developing world. She has also conducted extensive research on enhancing the reach and impact of the Multilateral Development Bank system. Before joining CSIS in September 2017, she was a senior consultant at the Economist Intelligence Unit (EIU). She worked closely with clients to design research and manage projects that included index building, quantifying qualitative variables, policy analysis, and strategies for investment and growth. EIU flagship projects include benchmarking indices like the Global Microscope on Financial Inclusion and the Latin America and Caribbean Infrascope project. Ms. Bandura is an economist with 18 years of experience in international development research, policy analysis, and project management. Before joining EIU, she was an economist at the International Labour Organization’s Washington office. In her previous capacity as a business manager at DAI’s Economic Growth Sector, she managed a $90 million private-sector development portfolio of projects in Africa, Asia, and Eastern Europe. She has also served as a policy analyst for the UN Development Program. Earlier in her career, she worked in the banking sector in Argentina. Ms. Bandura holds an MPA in international development from Harvard University’s Kennedy School of Government and a BA in economics from the Universidad Católica Argentina, Buenos Aires.

Sundar R. Ramanujam, a research associate with PPD at CSIS, focuses on the role of the private sector in global development challenges. His research and analysis extend to a range of subjects, including democracy and capacity building in frontier markets, structural reforms in emerging markets, and the impact of the digital revolution on sustainable development. Mr. Ramanujam has helped lead numerous working groups and research projects that studied how the United States can preserve the international liberal order by leveraging its bilateral agencies, long-standing relationships with allies and partners, and the effective use of the multilateral institutions. Mr. Ramanujam has been credited with several publications on development finance, the impact of digital revolution in the developing world, economic governance, quality infrastructure, and sustained private sector development in low-income countries, among other subjects. Some of his work on infrastructure and development finance has meaningfully impacted the outcome of the 2019 G20 Summit. Mr. Ramanujam has a personal research interest in understanding the role of constitutions and high courts in shaping the rule of law and the political economy. Before joining CSIS, he had worked for the renowned political scientist, Prof. Donald L. Horowitz, at the National Endowment for Democracy. He was also associated with the CSIS as a research intern for the Wadhwani Chair for U.S.-India Policy Studies during the summer of 2016. Mr. Ramanujam received his undergraduate training as an electrical engineer from Shiv Nadar University in India and holds a master’s degree in democracy and governance from the Department of Government at Georgetown University.
Annex 1: Definitions

- Legal identity (UN): Basic characteristics of an individual's identity (e.g., name, sex, place and date of birth) conferred through registration and the issuance of a certificate by an authorized civil registration authority following the occurrence of birth. In the absence of birth registration, legal identity may be conferred by a legally recognized identification authority. This system should be linked to the civil registration system to ensure a holistic approach to legal identity from birth to death. Legal identity is retired by the issuance of a death certificate by the civil registration authority upon registration of death.

- Proof of legal identity (UN): A credential (such as birth certificate, identity card, or digital identity credential) that is recognized as proof of legal identity under national law and in accordance with emerging international norms and principles.

- Digital identity (World Bank): A set of electronically captured and stored attributes and/or credentials that uniquely identify a person.

- Digital identification (ID) system (World Bank): An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.

- Digital identification (ID) system (USAID): A technology-enabled platform that establishes formal identification for populations to increase civic, economic, political, and social participation and provide community benefits. It also helps governments deliver the necessary citizen services (e.g., welfare programs, voter registration, licenses, and certifications). Specific systems currently vary in model, level of digital integration, trust and transparency, and registration.
Annex 2: Case Studies of Digital ID Systems: Estonia and India

**Estonia:** Since 1997, Estonia has slowly grown its digital ID system to provide public services online and further connect its society. 98 percent of Estonia’s 1.3 million people have a digital ID, and 67 percent use it frequently. Estonia’s e-identity or e-ID consists of ID cards, Mobile-ID, e-residency, and Smart-ID that provide its citizens and residents with easy ways to authenticate themselves and securely access e-services. The general ID card serves as a travel ID, national health insurance card, proof of identification for banks, digital signatures provider, i-voting card, and a medical and tax record manager. The physical card has a 384-bit ECC public key encryption chip with embedded files to prove identity. Mobile ID and Smart IDs are the SIM card and app extensions of the digital ID that allow citizens to use their phones to secure authentication and access financial services. Lastly, the e-residency system reimagines immigration and facilitates business and commerce among Estonian citizens, residents, and the wider EU and international community.

Overall, Estonia’s ID system provides access to 99 percent of all public services, e-tax filing systems, internet voting, KSI blockchain and cybersecurity, e-currency, e-health, and links to interoperable information systems known as the X-Road. Implementation of the ID system has cut billions in government and processing costs and saved Estonia approximately 2 percent of its economic output. The e-ID system is based on a decentralized IT system that connects hundreds of organizations, companies, and institutions that share data and information through X-Road. This decentralized system increases the security, sustainability, interoperability, and independence of platforms.

However, the system is not flawless. In 2017, Estonia experienced a large-scale cyberattack forcing 800,000 people to update and re-register their digital ID, although no information was compromised. Recently, Estonia created Data Embassies, which hold copies of Estonian databases in other countries—for example, the backup storage facility in Luxembourg, which serves as a safety measure in case Estonia experiences other cyberattacks. Currently, Estonia is rated second by Freedom House in terms of internet freedom and sets a global standard for an effective, decentralized digital ID.

**India:** In 2009, India created its first-ever national digital ID system that hosts the biometric data of those enrolled. Dubbed by Nobel Laureate Paul Romer as “the most sophisticated ID system in the world,” Aadhaar (which translates to “foundation” in Hindi) is today the world’s largest digital
ID system and is being used to reduce bureaucratic costs and address socioeconomic challenges. Using digital technology, Aadhaar brings approximately 1.25 billion people under its cover and grants them unique identification numbers, which are used to map the individuals with their biometric data. The functionality of Aadhaar ID has immensely transformed how the Indian government (and its economy) functions. Not only has Aadhaar already enhanced the Indian state's ability to track and collect taxes, but it has also proven to be quite helpful in reducing corruption and leakages while delivering welfare subsidies and public services. More than 10 years ago, 40 percent of India's population remained unregistered at birth while 30 percent could not read or write their names, locking them out of a host of services that needed proof of identity. Aadhaar changed this reality, making it easier for entities in the social sector (hospitals and universities) and the private sector (mobile service providers and financial institutions) to authenticate a customer's identity before delivering a service.

Despite having large enrollment numbers, Aadhaar is not without problems. Fraudulent enrollment and corruption have marred its launch and excluded citizens. The biometrics (fingerprints and iris scans) have not always rightly identified individuals, raising questions of reliability. Questions on data security remain unanswered, as individuals who have enrolled in the system face privacy risks and are left with little control over how much personal information can be easily accessed. A 2018 report found that any individual could access the entire database for just $7. In its present form, Aadhaar serves as a functional ID and authentication system. But with critical improvements to the ID governance policy, Aadhaar can take on more complicated and advanced ambitions. Specifically, changes are needed to address Aadhaar's data security and mismanagement concerns and to decrease the risk of cyberattacks on the system. There is also a need to realign social welfare policies so that the government more effectively leverages Aadhaar to achieve broader goals of economic development and poverty alleviation. With time and targeted policy changes, India can fully unlock the potential of Aadhaar and experience increased economic benefits, expand the formal labor market, and be a model case in financial inclusion for the development community.
Endnotes


5 Domeyer, McCarthy, Pfeiffer, and Scherf, “How Governments Can Deliver on the Promise of Digital ID.”

6 Ibid.


13 World Bank, “ID4D Global Dataset.”

14 White, Madgavkar, Manvika, Mahajan, Bughin, McCarthy, and Sperling, Digital Identification.

15 World Bank, “ID4D Global Dataset.”


FATF, FATF Guidance in Brief.

World Bank, “ID4D Global Dataset.”

Domeyer, McCarthy, Pfeiffer, and Scherf, “How Governments Can Deliver on the Promise of Digital ID.”


White, Madgavkar, Manvika, Mahajan, Bughin, McCarthy, and Sperling, Digital Identification.


Domeyer, McCarthy, Pfeiffer, and Scherf, “How Governments Can Deliver on the Promise of Digital ID.”


FATF, Guidance on Digital Identity.


FATF, FATF Guidance in Brief; Anita Mittal, Catalog of Technical Standards for Digital Identification Systems.
Many organizations around the world are tasked specifically to set up, monitor, and continuously update technical standards regarding how innovative technologies should be developed and deployed. These include international organizations (International Organization for Standardization [ISO], the International Electrotechnical Commission [IEC], ITU’s Telecommunication Standardization Sector [ITU-T], the World Wide Web Consortium [W3C], and the FATF); national organizations (in the United States, the American National Standard Institute [ANSI], the NIST, the U.S.-based International Committee for Information Technology Standards, and the U.S. Department of Homeland Security); and industry consortia (Biometric Consortium, Secure Identity Alliance [SIA], Center for Identification Technology Research [CITeR], and IEEE Biometrics Council).


FATF, Guidance on Digital Identity.
Domeyer, McCarthy, Pfeiffer, and Scherf, “How Governments Can Deliver on the Promise of Digital ID.”

Ibid.


White, Madgavkar, Manvika, Mahajan, Bughin, McCarthy, and Sperling, Digital Identification.

FATF, Anti-Money Laundering and Terrorist Financing.

FATF, Anti-Money Laundering and Terrorist Financing.


70 Some important U.S. government initiatives related to digital ID and digital financial inclusion include USAID’s Digital Strategy 2020–2024 (aimed at achieving and sustaining open, secure, and inclusive digital ecosystems conducive to broad-based, measurable development and humanitarian assistance outcomes and increased self-reliance); the U.S. Department of the Treasury’s National Strategy for Combating Terrorist and Other Illicit Financing 2020 (addressing the role of digital assets in criminal activities such as money laundering and terrorism finance); and DFC’s 2020–2025 strategy, DFC’s Roadmap for Impact (elevating innovation and technology across the agency’s portfolio).


75 “What Is India Stack?” India Stack, https://www.indiastack.org/about/.


77 FATF, Guidance on Digital Identity.


79 “Digital Ecosystem Fund: 2020 Activities,” USAID.

80 FATF, FATF Guidance in Brief.

81 NSCAI, Final Report.

82 “United Nations Legal Identity Agenda,” United Nations

83 Ibid.

Ibid.


O’Callahan, “What Happens When a Billion Identities Are Digitized?”

White, Madgavkar, Manvika, Mahajan, Bughin, McCarthy, and Sperling, Digital Identification.