ADBInstitute

ICRIER

policy brief

No. 2022-3 (August)

**Key Points**

- Digital identities have become popular worldwide given their potential to improve the efficiency, functionality, scalability, and coverage of government schemes and policies.
- A digital identity system must be situated within government to ensure inclusion, security, and sustainability.
- A robust accountability mechanism should be at the core of a digital identity system characterized by clearly designated roles and responsibilities for all parties involved, in tandem with a redressal mechanism to address logistical or systematic errors.
- Digital identity systems should be guarded with stringent cybersecurity and data privacy norms.
- Mandating digital identities for access to public services can lead to exclusion, especially in countries where internet penetration and digital literacy are relatively low.
- Mutual recognition of digital identities can enable cross-border economic integration and cooperation, though this needs to be supported by a robust and coordinated governance framework.


ISSN 2411-6734
DOI: https://doi.org/10.56506/XCNN8924



# The Emerging Era of Digital Identities: Challenges and Opportunities for the G20

Shiva Kanwar, Research Associate, Indian Council for Research on International Economic Relations
Aarti Reddy, Fellow, Indian Council for Research on International Economic Relations
Mansi Kedia, Senior Fellow, Indian Council for Research on International Economic Relations
Mayank Manish, Research Associate, Indian Council for Research on International Economic Relations

## 1. Introduction

An identity (ID) is a set of one or more attributes that allows an entity or person to be sufficiently distinguished or uniquely identified (GPFI 2018; ITU 2018). While the true nature of any identity is multifaceted, the functional purpose is to prove the uniqueness of an individual, ensure accountability, establish trust, and provide a point of reference for legal, social, and economic transactions.

IDs have been broadly classified as foundational or functional. A foundational ID is multipurpose and meant to provide identification for the general population, often forming the basis for various public and private sector transactions. A functional ID, on the other hand, is designed for a specific purpose (e.g., voter IDs, health records, tax ID numbers, social protection, ration cards, or driving permits) and usually covers a subset of the population. However, in many cases, these are accepted as proof of identity for broader purposes beyond their original scope, especially when robust foundational ID systems are not present. Further, a legal ID is one that is sufficient for proving the identity of an individual. Foundational IDs often serve as sovereign legal IDs but, in many instances, functional IDs are also accepted (AFI 2021; ID4D 2019; GPFI 2018; ITU 2018).

Identification is the process of establishing information about an entity or individual based on a set of attributes that uniquely describes them. Key parameters of an identity are uniqueness, recognition, and coverage. This entire process of registering, issuing, using, and maintaining identities is called the identity lifecycle and consists of several stages, starting from enrolling the identity data, storing it, establishing its validity and uniqueness, issuing credentials, verifying and authenticating,[1] and, finally, updating credentials (ID4D 2019; Access Now 2018; GPFI 2018; ITU 2018).

1 Verification is the process of comparing the credentials (e.g., a personal information number, a card) presented by an individual, with the stored credentials associated with their claimed identity. Authentication, a step further, is the process of ensuring that the person who claims an identity is the rightful owner of that identity, i.e., that they are really who they claim to be and they are the same person that the credentials associated with an identity were originally issued to.

A *digital identity* is one where most aspects of the system that enables it are accomplished digitally. While some digital identities are almost entirely digital, many are built upon pre-existing non-digital identification systems with only some aspects being digitalized. In these cases, digitalization can either replace existing mechanisms, or complement them. This policy brief focuses on digital identity systems administered by sovereign bodies (public, administrative, legal, and state-affiliated) that serve as foundational or functional identities.

### 1.1. *Evolution of Identity Systems: Progress in Technology and Increasing Centrality of Identification in Accessing Rights, Protections, and Services*

Governments and private bodies have maintained identification systems for a long time. Starting with censuses in ancient empires and personal identification numbers in the United Kingdom and Netherlands (1800s), various identification systems have been developed over time (Trulioo 2019). The need for a robust identification system was first established for legal and voting purposes. More recently, it has become integral to the access of various rights, protections, and public and private services. Digital systems have gained traction given their potential to improve efficiency, functionality, scalability, and coverage.

The process began with the incorporation of digital technologies to fulfill specific functions within identification systems. For instance, the United States Census Bureau purchased the Univac for storing and classifying demographic data in 1951 (Fabry 2016). Gradually, traditional methods of verification (usually based on physical checks such as matching an individual's face with an authenticated ID document with their credentials) were relegated to digital systems. The proliferation of the internet led to greater decentralization, integration, and portability of identification systems (Breckenridge 2018; Privacy International 2022b). In the past 2 decades, countries have begun developing ID systems that are based on digital infrastructure, as opposed to the incremental digitalization of existing identity systems. The next section summarizes country approaches to development of digital identities.

## 2. Digital Identities: Approaches and Design

### 2.1 *Overview*

Country approaches to the development of digital identification systems are unique in scope, timing, implementation and governance frameworks. In Table 1, we discuss the digital identity programs of 10 countries, both members and non-members of the G20, geographically diverse with varying levels of economic prosperity, have different approaches to digital identity systems and at different stages in their design and implementation.

### 2.2 *Case Studies*

#### 2.2.1 Kenya: Of Precedents, Privacy, and Data Protection

The National Integrated Identity Management System (NIIMS), popularly known as Huduma Namba (service number in Swahili) is Kenya's biometric digital identity program. It was established in 2019 under section 9A of the Registration of Persons Act, 1949 wherein it was introduced via the Kenyan Statute Law (Miscellaneous Amendment) Act No. 18, 2018 (CIS 2020). It was developed to create, maintain, manage and operate a national population register as a single source of personal information for all Kenyan citizens and registered foreigners resident in Kenya; and to assign a unique national identification number to every person in the register (Privacy International 2022a).

The data to be collected for the NIIMS included biometric data such as fingerprints, voice waves, and iris and retina patterns, along with DNA and GPS data (Privacy International 2022d). Consequently, three petitions[2] were filed before the Kenyan High Court on the grounds that, *inter alia*, NIIMS called for the collection and processing of large amounts of sensitive personal data in the absence of protection law, and required compulsory registration which, coupled with linking digital identity with welfare services, could potentially exclude marginalized groups. The Court combined these petitions (Nubian Rights Forum & 2 Others v Attorney General & 6 Others 2020) and issued a crucial interim ruling before the final judgment (Bhatia 2020; Research ICT Africa and CIS 2021; Baliga 2022).

2 By the Nubian Rights Forum, the Kenya Human Rights Commission, and the Kenya National Commission on Human Rights.

## Table 1: Overview of Digital Identity Initiatives Across Countries

| Country | Nature of Digital Identity | Purpose | Implementation and Regulatory Framework | Impact Assessment Conducted |
|---|---|---|---|---|
| India | India has the largest foundational digital identity program in the world: Aadhaar. It has been issued to more than a billion residents and serves as the primary identity for most people in the country. | The program was originally designed to improve efficiency in the distribution of welfare subsidies but evolved in scope for multiple purposes including opening of bank accounts, subscription to telephone and internet services, access to food subsidies, etc. | The Unique Identification Authority of India manages the enrollment, authentication, and implementation of Aadhaar. It is also the foundation for multiple new IDs such as the Digital Health ID. | Aadhaar is the foundation of the Government's financial inclusion program. The Aadhaar Enabled Payment System is a bank-led model that allows online interoperable financial inclusion transactions.<br>Recently, the State of Aadhaar report and the Report of the Comptroller and Auditor General of India on the "Functioning of Unique Identification Authority of India" found that, while Aadhaar provides an easy and efficient method of verification, it also leads to exclusion. There are high levels of authentication failure (measured at 49% in a few states). |
| US | The primary government identities (for both federal and state) are paper-based. Recently some states have launched digital driver's license/ mobile IDs. | It replaces the physical driver's license as used for identification for a variety of activities in a particular state. | In most states, the Department of Motor Vehicles issues and manages the identity that is being developed with the help of technology company IDEMIA following industry standards for digital IDs.<br>The federal government has yet to become a digital identity provider. Public–Private-Partnerships such as Electronic Authentication Partnership and the Trust Framework Solutions program fill the gaps for online verification of individual identity. | The use of digital identities in states is very recent and has yet to reach a threshold level to measure impact. Overall, the patchy system of identity management in the federal government has led to fraudulent claims worth $36 billion under the US CARES Act (Penzenstadler 2022). This paved the way for the Improving Digital Identity Act 2021 to develop secure methods for government agencies to validate identity while protecting the privacy and security of individuals and supporting interoperable verification across the public and private sectors. |
| Saudi Arabia | The National Identity card is a foundational digital identity and is mandatory for all citizens and residents of Saudi Arabia aged 15 and above (My.Gov.Sa. 2022b). | The "Digital ID" is the electronic version of the national identity card.<br>It can be used to access government online services, verify identity with banks and telecom operators, and as a travel document within the Gulf Cooperation Council member states (My.Gov.Sa. 2022a; Saudi Gazette 2021). | It is governed by the Ministry of Interior's instructions on National ID. | While the nation's government has not conceded that their initiative may be facing challenges common to all digital identities (such as data protection, privacy etc.), some studies have raised concerns regarding gender discrimination, and exclusion due to requirements for collection of biometric data (SMEX 2021). |
| Brazil | The National Civil Identification Program launched in 2017 was Brazil's first attempt to combine multiple identities and create Brazil's National Identification Document. In 2020, the government combined the social security card and driver's license to create a digital identity operationalized using an app. | This combined ID can address the problem of multiple federal and state government IDs (individuals could own up to 27 IDs) that led to credit card fraud and breach of personal data in the country. The initial goal was to reduce electoral fraud. | Issued by the Superior Electoral Tribunal (TSE) and Sepro, the federal data processing service, which developed this app. It will be printed by the national mint and will use Individual Taxpayer Register as the basis of identification. The database will be managed by TSE. | Digital identities (National Identification Document, Menu ID, Blockchain device ID,) have helped unlock efficiencies in e-government services, enabled financial inclusion and also shown promise for online education. |

*continued on next page*

**Table 1** *continued*

| Country | Nature of Digital Identity | Purpose | Implementation and Regulatory Framework | Impact Assessment Conducted |
|---|---|---|---|---|
| Indonesia | Indonesia, one of the early adopters of digital identities, introduced e-KTP (Kartu Tanda Penduduk- elektronik), a nationwide foundational digital identity in 2011. It contains unique biometric data of citizens (ADB 2016). | The program was started to combat voter fraud and terrorism but is currently the predominant ID for multiple purposes (e-voting, e-sign). | The initiative to implement a single unique identity number was formally established in the Senate Regulation Number VI/ MPR/2002. Act No. 23, 2006, Government Regulation Number 37, 2007 and the presidential Regulations no. 26 & 35 form the legislative basis of the e-KTP program. | As of 2021, more than 98% of Indonesia's population possessed an e-KTP. By the end of 2020, around 2,819 government and private institutions, including 1,177 banks, had access to demographic data of citizens from this database (Salyanty et al. 2020). |
| PRC | The PRC does not have a nation-wide digital identity yet though plans have been stated to roll out a digital ID in 2022. The PRC Ministry of Public Security has been testing digital ID technologies since 2018 and has introduced virtual ID services in 15 major cities, giving residents the option to use virtual IDs for hotel bookings and ticketing and banking, using facial recognition for authentication during such interactions (NFCW 2022; South China Morning Post 2022). | Multipurpose digital identity, from identity verification to booking tickets, banking services, hotel bookings. | The PRC's Personal Information Protection Law concerning data protection went into effect on 1 November 2021. The law governing resident identity card will need to be amended to recognize digital identities as well as incorporate privacy concerns (National People's Congress of the People's Republic of China 2022). | Not applicable |
| Estonia | Estonia's foundational eID and digital signature has been around since 2002 and is mandatory for all citizens. | It is mandatory as legal identification and used for various purposes such as digital signatures, internet-based voting, as a national health insurance card, proof of identification when logging into bank accounts, and for submitting tax claims (E-Estonia 2022b). | The system is designed and operated by a group of private companies, and overseen by the national Police and Border Guard Agency (PGBA). The PGBA is also responsible for verification for new users. The data held by the government are decentralized and duplicated via data embassies.[c] | 99% of Estonians have the ID card which allows them to use the eID.[a] While the system has generally been assessed as successful, security threats have and continue to pose challenges,[b] Estonia's digital identity system has been a pioneer and continues to innovate (e.g., use of cryptographic hashing functions for linking data,[d] building trust,[e] promoting security-related R&D). |
| Kenya | The Huduma Namba is a foundational digital identity | It is a multipurpose digital Identity that provides every citizen or resident of Kenya with a unique national identification number; it can be used to access government services, for Subscriber Identity Module registration, as an identification document for travel in the East African region, etc. | The Huduma Namba was established under section 9A of the Registration of Persons Act of 1949 via the Kenyan Statute Law (Miscellaneous Amendment) Act No. 18 of 2018, enacted in January 2019. | Huduma Namba was challenged before the Kenyan High Court for being launched in the absence of data protection law and without a data impact assessment. The scheme rollout has been halted until the government conducts a data protection impact assessment. |

*continued on next page*

**Table 1** *continued*

| Country | Nature of Digital Identity | Purpose | Implementation and Regulatory Framework | Impact Assessment Conducted |
|---|---|---|---|---|
| UK | The UK's One Login system, announced in 2021, is a single sign on service to access various platforms. The previous system, UK Verify, was discontinued in 2021 (Diginomica 2021; Jones 2021). | The One Login system is intended to streamline the use of multiple functional IDs many of which are already using digital infrastructure to some extent. | The One Login system will be coordinated by the Government Digital Services and co-designed with Whitehall departments. It is intended to be largely government-built and government-owned. The distributed approach of the proposed model, however, is intended to mitigate some of the privacy risks that are likely to emerge from a centralized scheme. Consultations for a digital identity and attributes framework are underway. | The previous system, UK Verify, (launched in 2013, and live in 2016) was a federated identity system.[f] The Government Digital Service, was estimated to have spent over £130 million the development of Verify, but uptake and integration remained subpar.[g] The Verify program was eventually dropped completely in 2021.[h] The new One Login system takes a more centralized approach with identity management is done by a single entity and shared with other departments rather than managed by each department separately. |
| Italy | Italy's Public Digital Identity System (SPID), allows online access to services based on personal credentials (username and password). | Launched in 2016, the SPID, allows individuals and businesses to access services of the public administration and private adherents, based on personal credentials (username and password). | The SPID is a public–private partnership, with nine identity providers as of 2021, with the Italian Postal Service, a public entity, having the highest market share (83%). | It has been used most intensively for accessing the national retirement system and interactions with public administration. It is also used to access federal and state level benefits. There has been increase in uptake in recent years, with over 23 million users as of August 2021. Adoption rates are uniform by gender, but low for older population.[i] |

PRC = People's Republic of China, UK = United Kingdom, US = United States.

Notes:

[a] The e-ID can be used via a state-issued ID card, mobile ID, or the Smart-ID application. The card has a chip carrying embedded files and uses a 384-bit elliptic-curve cryptography public key encryption, to serve as ID proof in a digital environment. The Mobile-ID system is based on a special mobile Subscriber Identity Module card, which stores private keys and a small application supporting authentication and signature functions, which users request from the mobile phone operator.

[b] Estonia's digital infrastructure saw its most serious challenge in 2007, when Russian hackers broke into numerous systems and caused extensive disruption. The digital ID system has seen more recent attacks, including a breach this summer of some 300,000 document photos and a vulnerability found in the circuitry of physical ID cards in 2017 that required blocking the digital certificates of about 760,000 of them (Fast Company 2021).

[c] These are data centers that are located outside Estonia, but are under its full control with the same rights as physical embassies (e.g., immunity) (Privacy International 2022c).

[d] The X-Road system, upon which Estonia's digital identity system is based, is an open-source data exchange layer solution that facilitates the exchange of information between organizations over the Internet. It is a centrally managed distributed integration layer between information systems which provides a to produce and consume services that is standardized and secure. It ensures confidentiality, integrity and interoperability. Its use of cryptographic hash functions for linking data items to each other, is similar to blockchain technology (Kivimäki 2018; e-Estonia 2022a).

[e] Estonians can see who has accessed their information, and hold them accountable. Authorities have promoted transparency about system breaches and emphasized communication with the public. There are educational programs to promote digital literacy and understanding of cyber threats. (Stone 2021).

[f] Federated identity systems allow for the linking of an individual's identity across multiple separate identity management systems.

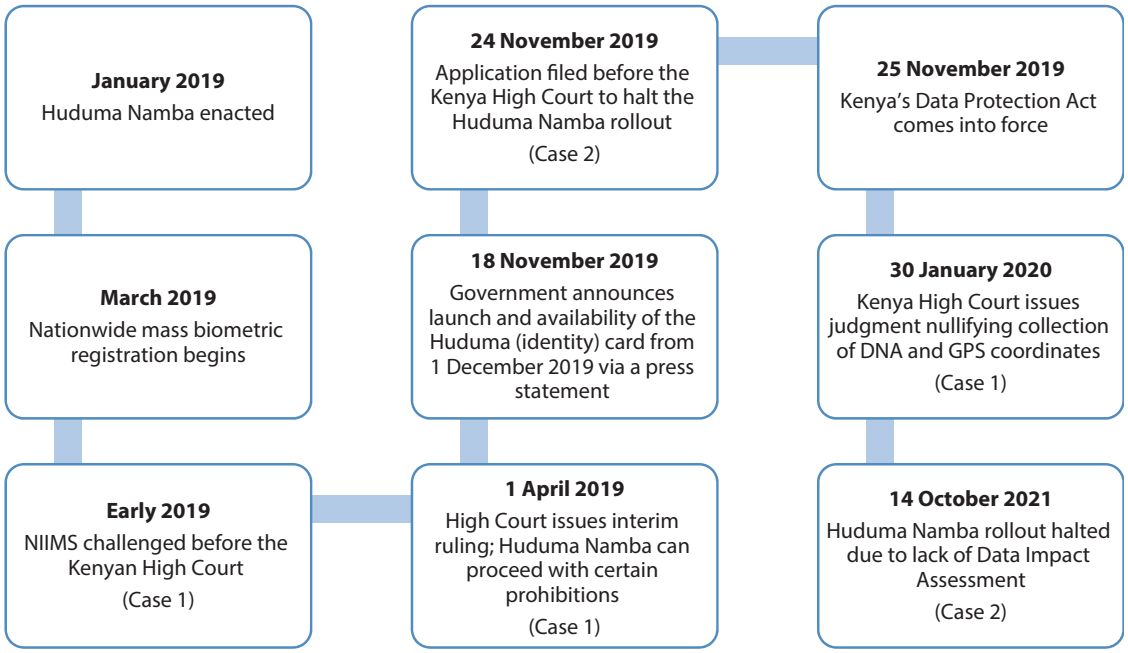
[g] By 2018, only 2.9 million people signed up and the system was used in only 18 public services in 2018. By late 2021, there were still 44 different sign-in methods and 91 different ways for people to set up various accounts to access different services on Gov.uk. (Cabinet Office announcement 2022).

[h] In 2018, the government announced that it would be transitioning this to a private sector led model, in the backdrop of various departments having lost confidence in the system and being unwilling to fund further development. The revenue and customs department (HMRC) had begun developing a new version of its existing Government Gateway system (which, by 2021 had 16 million users, more than double that of the Verify program). The National Health Service (NHS) began developing its own identity system due to concerns of Verify not being secure enough for health services. The Verify program was eventually dropped completely in 2021 (Fishenden and Mather 2022).

[i] 87% of people 18–24 years of age are SPID users, while only 34% of 65–74-year-olds, and 14% of people over 75.

Source: Authors.

**Figure 1: Tracking Kenya's National Integrated Identity Management System**




NIIMS = National Integrated Identity Management System, GPS = global positioning system.

Source: Bingham 2021; Baliga 2022; Privacy International 2022a; Privacy International 2022d.

The interim ruling stipulated that while the Government could proceed with Huduma Namba, it was prohibited from mandating participation in the program. Subsequently, the Government announced the launch of Huduma Namba cards via a press statement and Kenya's Data Protection Act also came into force. Roughly a month after the enactment of the Data Protection Act, the High Court delivered its judgment wherein it nullified the mandate in NIIMS to collect DNA and GPS coordinates declaring it as "intrusive and unnecessary" (Baliga 2022; Privacy International 2022d).

Huduma Namba faced another challenge[3] in the High Court on grounds that the program was being launched without a data impact assessment as required under the Data Protection Act. The Court upheld the retrospective application of the Data Protection Act on the Huduma Namba and halted the programs rollout until the government conducted a data protection impact assessment (Bingham 2021).

This precedent will have an overarching impact on the future of digital identities, especially as a step forward in the ongoing fight for privacy in centralized digital identity systems (Privacy International 2022g). It emphasizes the need for substantial safeguards in the implementation of a centralized digital identity program. While the court-mandated data protection impact assessment has not yet concluded, Kenya has exemplified the significance of issues like privacy and data protection in digital identity systems (World Economic Forum 2022).

### 2.2.2 United States: Of Integration

The US-backed identity system is a patchwork of processes managed by the federal government, states, and local agencies. The Social Security number and state-issued driver's license are the most important elements of the country's identity system, though neither is universal or digital. Most recently, several state governments have launched their digital/mobile driver's license, the adoption of which has tripled in 2021 (Appleinsider 2021). This is now being used for several age-based transactions such as purchasing alcohol and certain medications, as well as at financial institutions. The Social Security Administration is also working toward

3 Petition filed by the Katiba Institute.

the implementation of electronic Content Based Social Security Number Verification or eCBSV (Ssa.Gov 2022). However, a larger overhauling of the country's digital identity system is being planned and implemented through the Improving Digital Identity Act of 2021, placed within the executive office of the President.

The National Institute Standards and Technology will develop a standards framework for digital identity verification to guide federal, state, and local governments in selecting their digital identity solutions (Magrath 2022). It also provides for a budget to help states upgrade systems used to issue drivers' licenses and other forms of digital ID credentials (Hersey 2021). At the heart of this change lies a recognition that there is no substitute for the unique role governments can play in conferring a legal identity (Better Identity Coalition 2018). This is in sharp contrast to the government's earlier efforts with public–private partnerships to fill the gaps on verification. Systemic lacunae and fragmentation result in hefty identity theft amounting to $712.4 billion lost in 2020 (Inscoe 2021; Insurance Information Institute 2022). The envisioned identity program will prevent fraud and support unified public support on education, health and unemployment, that were challenges faced by the country during the novel coronavirus (COVID-19) pandemic.

### 2.2.3 India: Of Efficiency, Errors, and Exclusion

India's foundational digital identity, Aadhaar ("foundation" in Hindi) remains the largest biometric digital identity program in the world, with over a billion cards issued to residents. The identity system is used for delivering subsidies, creating bank accounts, and buying mobile Subscriber Identity Module cards. The identity has truly become multi-purpose, despite the governing legislation and India's apex court declaring that the identity system should only be a voluntary program used for welfare distribution. The 12-digit unique identification number is connected to demographic information and biometrics of individuals (iris scan and fingerprints). Enrolment, implementation, and authentication is managed by the Unique Identification Authority of India (UIDAI). The biometric and demographic details are stored on central servers of UIDAI. Aadhaar is now on its way to becoming the foundation of e-governance with multiple new digital initiatives such as e-Kisan, e-Shram, and the National Health ID being linked or built upon it, for which the robustness of Aadhaar becomes critical, a system that functioned in a legislative vacuum for the first half-decade of its existence.

According to the State of Aadhaar report (Totapally et al. 2019), individuals use Aadhaar to access multiple services, both public and private. Despite widespread use and utility, a significant number of Indians face challenges such as exclusion or denial of essential services due to authentication errors with Aadhaar. The Comptroller and Auditor General of India, a constitutional body, found authentication errors to be as high as 49% in some states. It also found significant levels of duplication in the system, despite the claim of uniqueness (CAG 2022). While Aadhaar has served as the primary identity both digital and physical for most Indians, the large number of excluded citizens (due to authentication errors and other challenges) should be a significant source of concern (Privacy International 2022b). Moreover, reported instances of data mismanagement call for better governance of the Aadhaar program (Jain 2019).

### 2.2.4 Italy: Of Successful Public–Private Partnership

Italy's Public Digital Identity System (SPID), which was launched in 2016, allows individuals and businesses to access services of the public administration and private adherents, based on personal credentials (username and password). Initial issuance is based on existing Italian identification (identity card, passport, or driving license), along with health card (*tessera sanitaria*) or tax code card (*codice fiscal*), e-mail address, and mobile phone number. After the initial verification process, the ongoing usage of the system has three levels of authentication depending on the service being accessed, with Level 1 requiring only a username and password. The SPID is a public–private partnership, with nine identity providers as of 2021, with the Italian Postal Service, a public entity, having the highest market share (83%). Italy also launched the CIE, an Electronic Identity Card with a near-field communication-enabled chip, in late 2015. Both the CIE and SPID are notified to the European Commission and regulated by the Electronic Identification, Authentication and Trust Services (eIDAS) European scheme (SPID 2022a, 2022b).

SPID has been used most intensively for accessing the national retirement system, as well as for interactions with public administrations such as for tax payment. It is also being used to obtain federal and state level benefits for which identity verification is required (e.g., child benefits, family allowance, educational allowance, housing subsidies). The government had required that all public authorities and bodies make their

services available through SPID and other electronic IDs by October 2021. Approximately 28% of all public administrations in Italy, however, were not yet part of the system in November 2021. While growth was slow initially, user adoption has seen rapid uptake in more recent years, with over 23 million users by August 2021. By October 2021, 43% of Italian citizens had the digital identity. Voucher campaigns to incentivize uptake, development programs and a dedicated digital transformation team have been credited for this. The provision of interoperable products by various private companies has boosted user take-up. Adoption rates have been relatively uniform by gender, but remain low for older populations (MEF 2021; Namirial 2021; SPID 2022b).

### 2.3 *Key Messages*

The primary objective of all national digital identities is to facilitate access to public services. While nations focus on the potential benefits of these initiatives, their risks should also be acknowledged, especially as developing digital identity frameworks often involves governments working together with third parties. In such cases, a clear delineation of roles, responsibilities, expectations, and liabilities is necessary to establish accountability.

Challenges faced by digital identity systems only increase with scale. Evidenced by the UIDAIs report (UIDAI 2012),[4] which acknowledges an occasional false positive to arise in the system. Considering the scale of the scheme and India's population, the number of actual errors in the system can be considerable (Privacy International 2022b). The latest audit report on Aadhaar does point toward these gaps (CAG 2022).

Further, mandating digital identity for accessing government services can lead to exclusion as access to public services can be denied due to lack of the ID (Privacy International 2022e). Logistical or technical barriers such as discrepancies in the system, managing accurate authentication, and lack of infrastructure can make enrollment and verification for digital identities difficult, especially for the elderly and manual laborers.[5]

National digital identity initiatives involve collecting and storing sensitive personal information on a large scale; balancing this aspect against the right to privacy that flows into protection of data of individuals is imperative (Privacy International 2022f). Kenya's example enforces the necessity of data protection regulations and privacy safeguards, for better implementation of digital identity systems. National digital identity systems should also account for cybersecurity risks that can compromise sensitive personal data of a large population (Privacy International 2017; BBC News 2022). The severity of such breaches is amplified with national digital identity systems that often store biometric data, which cannot be easily rectified.

Finally, unique identity elements have long been associated with fears of surveillance. This now extends to digital identities with apprehensions of these initiatives—and the sensitive data they contain, such as biometrics—being used as tools of surveillance.[6] This trepidation extends to both governments and malicious third parties.

## 3. Exploring Cross-Border Digital Identities

Section 2 illustrates how identity and consequently digital identity landscapes are designed within the specific cultural, legal, and administrative contexts of every country. The diverse nature of digital identity systems makes harmonization an insurmountable task and perhaps unnecessary. Cross-border digital identity systems may not mean the creation of a harmonized global digital identity system but one that allows for the recognition and use of one country's digital identity in another. In other words, it need not be the same or similar digital identity across countries; it just needs to be trusted, i.e., recognized across borders. There can be several advantages to cross-border digital identity systems of the kind referred to above. All cross-border movement of goods, capital and people can be made more efficient, safe, and inclusive with the use of cross-border digital identity systems. For instance, it can enable smoother travel and migration across borders, easier cross-border electronic transactions and better access to services such as opening bank accounts and accessing medical records across borders (ID4D 2019; IDID 2022; Cooper 2022).

4 Titled "Role of Biometric Technology in Aadhaar Enrollment".
5 This is a widespread concern acknowledged by Kenya's High Court (Nubian Rights Forum & 2 Others v Attorney General & 6 Others 2020), research reports in Saudi Arabia (SMEX 2021), and the CAG report on Aadhaar in India to name a few (CAG 2022).
6 Several national digital identity initiatives have been subject to this concern, for instance, in the PRC, Saudi Arabia (SMEX 2021), and India's Aadhaar.

The European Union's (EU) eIDAS regulation is a successful example of a cross-border digital identity system. Enforced in September 2018, the eIDAS regulation created a framework for electronic identification to better enable service delivery across the EU. Digital identities of EU member states compliant with the regulation can be used to access public services region-wide. This system of mutual recognition allows nations to implement their own digital identity systems while enabling citizens to use their digital IDs (European Commission 2018, 2022a, 2022b).

Digital identities in some countries are also recognized as a valid travel document in lieu of a passport, such as MERCOSUR (the Southern Common Market, known as MERCOSUR for its Spanish initials) countries in Latin America,[7] and Kenya, Rwanda and Uganda in East Africa. Several other regional blocs, i.e., the African Union,[8] the Economic Community of West African States,[9] and the East African Community (EAC),[10] are also exploring mutual recognition of digital identity systems (ID4D 2019; ID4D, EAC & the World Bank Group 2021).

However, these instances have a common denominator; these nations all enjoy regional proximity and strong diplomatic relations and partnerships, which is a prerequisite to working toward a system of mutual recognition of digital identities. Facilitating the widening of this network and including mutual recognition of digital identities in regional trade and economic partnership agreements must remain the pursuit of multilateral platforms such as the G20. A recent policy brief analyzed 305 Regional Trade Agreements in force and notified the World Trade Organization (up till June 2020) that none included digital identities (Norberg, Ganne and Hewett 2020). However, the recent Digital Economy Partnership Agreement between Chile, New Zealand, and Singapore aims to facilitate digital trade using mutually recognized, safe, and secure digital identities (DEPA 2020). Cross-border digital identity arrangements will have to be supported by robust governance frameworks, perhaps through an existing multilateral secretariat that enables its implementation and regular monitoring.

# 4. Policy Recommendations

The G20 recently noted the significance of digital identities in the G20 Digital Identity Onboarding report and the G20 Rome Leaders' Declaration, 2021. The report emphasized the prominence of a digital identity, particularly for marginalized sections of society, toward accessing basic services and participating in society. It also recognized the central role that governments play in the digital identity landscape. The G20 declaration[11] emphasized "secure, interoperable and trusted digital identity solutions" that could provide access to services while balancing data protection and privacy concerns, and committed to pursuing digital identity tools that could be used in emergency situations. Considering the recent emphasis on the issue by the G20, this policy brief outlines the following recommendations to facilitate an inclusive, sustainable, and secure digital identity framework for countries across the world (World Bank 2021).

### 1) On Formulating a Digital Identity

With the world rapidly moving toward a digital landscape, digital identities are imminent. They can help the marginalized obtain legally recognized IDs, enable participation in previously unavailable economic opportunity, and facilitate smoother operation and delivery of public services. Countries that do not yet have a national digital identity program in implementation or development should begin to systematically consider how digitalization can improve the efficiency and inclusion of their current identity management systems and services that are tied to it.

### 2) On the Role of Governments

Digital identity frameworks are often the result of cooperative efforts between governments and third parties, such as private companies and not-for-profit organizations. While such public–private partnerships have proven beneficial and effective in many cases, a well-functioning system must be situated within the government with a robust accountability framework that appropriately balances the needs of an inclusive, sustainable, and secure digital identity framework.

7 Member States Argentina, Brazil, Paraguay and Uruguay, and Associated States Bolivia, Chile, Colombia, Ecuador and Peru.
8 The African Union held a consultation on a continental digital ID interoperability framework. Referenced at https://dig.watch/updates/au-holds-consultation-continental-digital-id-interoperability-framework.
9 The Economic Community of West African States ID card.
10 The Democratic Republic of the Congo, the Republics of Burundi, Kenya, Rwanda, South Sudan, Uganda, and the United Republic of Tanzania.
11 G20 Rome Leaders' Declaration, Rome, 31 October 2021, para 51.

### 3) On Governance and Accountability

Digital identity systems should have clearly defined roles and responsibilities of all parties involved, especially third parties that may have access to individual data. Accountability mechanisms should be created not only to achieve desirable socio-economic outcomes but also to prevent system abuse. Digital identities should not be mandated for access to public services and relief programs and schemes; this can lead to exclusion of the most vulnerable parts of the population. No system created is infallible—authentication, verification, logistical, or systematic errors can creep into any digital system. A well-designed redressal mechanism should be created to mitigate these situations. Digital identity programs should be free from discrimination and promote inclusion by design, particularly for vulnerable and marginalized groups.

### 4) On Data Protection and Privacy

Data protection and privacy should be a foundational aspect of digital identity systems. Countries should ensure that a robust data protection system is in place before enacting a digital identity program. Such programs should also undergo rigorous data protection impact assessments periodically to determine their validity. Additionally, the purpose for collection and use of data should be clearly defined and assessed in order to balance the need to collect and store sensitive personal data, and the digital identity program benefits. Transparency is key: only necessary information should be shared for each transaction, with users having the right to see how their information is being used.

### 5) On Cybersecurity and Disclosure

Digital identity programs should incorporate stringent security measures against tampering, unauthorized access, and theft and misuse of data. Further, the policy and legal framework sustaining the program should incentivize disclosure and reporting of vulnerabilities and breaches. This would allow for a more transparent system and help plug in gaps in security. Likewise, in case of a data breach, all affected parties including individuals should be notified. This disclosure requirement will allow citizens to know if or when their data are compromised and enable them to protect themselves.

## References


Access Now. 2018. *National Digital Identity Programmes: What's Next?*. https://www.accessnow.org/cms/assets/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf (accessed 13 May 2022).

Alliance for Financial Inclusion (AFI). 2021. *Policy Model for Digital Identity and Electronic Know Your Customer (E-KYC)*. https://www.rfilc.org/wp-content/uploads/2021/09/Policy-Model-for-Digital-Identity-and-Electronic-Know-Your-Customer-e-KYC.pdf (accessed 13 May 2022).

Appleinsider. 2021. *30 States Working on Digital Drivers Licenses, TSA Will Allow Them Soon*. https://appleinsider.com/articles/21/12/21/30-states-working-on-digital-drivers-licenses-tsa-will-allow-them-soon (accessed 13 May 2022).

Asian Development Bank (ADB). 2016. *Identity For Development in Asia and The Pacific*. https://www.adb.org/sites/default/files/publication/211556/identity-development-asia-pacific.pdf (accessed 13 May 2022).

Baliga, V. 2022. *Kenya's Huduma Namba: Ambition Fraught with Risk - Privacy Protection - South Africa*. https://www.mondaq.com/southafrica/privacy-protection/960004/kenya39s-huduma-namba-ambition-fraught-with-risk (accessed 13 May 2022).

BBC News. 2022. South Korean ID System to Be Rebuilt from Scratch. *BBC News*. 14 October. https://www.bbc.com/news/technology-29617196 (accessed 13 May 2022).

Better Identity Coalition. 2018. *Better Identity in America: A Blueprint for Policymakers*. https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5b4fe83b1ae6cfa99e58a05d/1531963453495/Better_Identity_Coalition+Blueprint+-+July+2018.pdf (accessed 13 May 2022).

Bhatia, G. 2020. *Notes From a Foreign Field: The Kenyan High Court's Judgment on The National Biometric ID System*. https://indconlawphil.wordpress.com/2020/02/08/notes-from-a-foreign-field-the-kenyan-high-courts-judgment-on-the-national-biometric-id-system/ (accessed 13 May 2022).

Bingham, L. 2021. *"The Cart Before The Horse" – A Kenyan Court Just Quashed A USD 95M Biometric Digital ID Project*. https://www2.law.temple.edu/voices/the-cart-before-the-horse-a-kenyan-court-just-quashed-a-usd-95m-biometric-digital-id-project/ (accessed 13 May 2022).

Breckenridge, G. 2018. *A Brief History of Digital Identity*. https://medium.com/humanizing-the-singularity/a-brief-history-of-digital-identity-9d6a773bf9f5 (accessed 13 May 2022).

Cabinet Office Announcement. 2022. *New One Stop Service for GOV.UK Unveiled*. https://www.gov.uk/government/news/new-one-stop-service-for-govuk-unveiled (accessed 10 June 2022).

Centre for Internet and Society (CIS). 2020. *GOVERNING ID: Kenya's Huduma Namba Programme*. https://cis-india.org/internet-governance/digital-id-kenya-case-study (accessed 13 May 2022).

Comptroller and Auditor General of India (CAG). 2022. *Report of the Comptroller and Auditor General of India on Functioning of Unique Identification Authority of India*. https://cag.gov.in/webroot/uploads/download_audit_report/2021/24%20of%20 2021_UIDAI-0624d8136a02d72.65885742.pdf (accessed 13 May 2022).

Cooper, A. 2022. *Cross-Border Digital Identity and Onboarding*. https://thepaypers.com/expert-opinion/cross-border-digital-identity-and-onboarding--1242279 (accessed 13 May 2022).

Diginomica. 2021. *British Government – Once Again – Aims for 'One Login for Government*. https://diginomica.com/british-government-once-again-aims-one-login-government (accessed 16 May 2022).

Digital Economy Partnership Agreement (DEPA). 2020. Digital Economy Partnership Agreement. https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement (accessed 10 June 2022).

Digital Watch Observatory. 2021. *AU Holds Consultation on Continental Digital ID Interoperability Framework*. https://dig.watch/updates/au-holds-consultation-continental-digital-id-interoperability-framework (accessed 10 June 2022).

E-Estonia. 2022a. Data Embassy - E-Estonia. https://e-estonia.com/solutions/e-governance/data-embassy/ (accessed 13 May 2022).

———. 2022b. ID-Card - E-Estonia. https://e-estonia.com/solutions/e-identity/id-card/ (accessed 13 May 2022).

European Commission. 2018. *Cross-Border Digital Identification for EU Countries: Major Step for a Trusted Digital Single Market*. https://digital-strategy.ec.europa.eu/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market (accessed 13 May 2022).

European Commission. 2022a. *European Digital Identity*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en (accessed 13 May 2022).

———. 2022b. *Discover eIDAS*. https://digital-strategy.ec.europa.eu/en/policies/discover-eidas#:~:text=Professional%20services%20sector-,What%20is%20eIDAS%3F,country%20they%20take%20place%20in (accessed 13 May 2022).

Fast Company. 2021. *This Country Moved Its Government Online. Here's Why That Wouldn't Fly in The U.S.*. https://www.fastcompany.com/90671437/estonia-digital-citizenry-evoting (accessed 13 May 2022).

Fabry, M. 2016. The Story Behind America's First Commercial Computer. *TIME*. https://time.com/4271506/census-bureau-computer-history/. (accessed 13 May 2022).

Fishenden, J. and A. Mather. 2022. *Government Gateway At 20 – Looking Back at the UK's Most Successful Digital Identity System*. https://www.computerweekly.com/opinion/Government-Gateway-at-20-looking-back-at-the-UKs-most-successful-digital-identity-system (accessed 13 May 2022).

G20 Rome Leaders' Declaration. 2021. *G20 Rome Leaders' Declaration*. http://www.g20.utoronto.ca/2021/211031-declaration.html (accessed 10 June 2022).

Global Partnership for Financial Inclusion (GPFI). 2018. *G20 Digital Identity Onboarding*. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf (accessed 13 May 2022).

Hersey, F. 2021. *US Congressmen Reintroduce Sweeping Digital ID Bill*. https://www.biometricupdate.com/202107/us-congressmen-reintroduce-sweeping-digital-id-bill (accessed 13 May 2022).

Identification For Development (ID4D). 2019. *ID4D Practitioner's Guide*. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf (accessed 13 May 2022).

Identification For Development (ID4D), East African Community (EAC) & the World Bank Group. 2021. *Study of Options for Mutual Recognition of National IDs in the East African Community*. https://documents1.worldbank.org/curated/en/337501535031584335/pdf/129621-ACS.pdf (accessed 13 May 2022).

Identification For Development (ID4D). 2022. *Mutual Recognition of IDs Across Borders: Practitioners Guide*. https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0 (accessed 13 May 2022).

Inscoe, S. 2021. *US Identity Theft: A Stark Reality*. https://aite-novarica.com/report/us-identity-theft-stark-reality (accessed 10 June 2022).

Insurance Information Institute (III). 2022. *Facts + Statistics: Identity Theft and Cybercrime*. https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#:~:text=Additional%20resources-,The%20scopr%20of%20identity%20theft,to%20%24712.4%30billion%20in%202020 (accessed 13 May 2022).

International Telecommunication Union (ITU). 2018. *Digital Identity Roadmap Guide*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-DIGITAL.01-2018-PDF-E.pdf (accessed 13 May 2022).

Jain, M. 2019. *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*. The Henry M. Jackson School of International Studies, University of Washington. https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/ (accessed 13 May 2022).

Jones, A. 2021. *Is The UK Ready for The Future of Digital ID?*. https://www.raconteur.net/digital/is-the-uk-ready-for-the-future-of-digital-id/ (accessed 13 May 2022).

Kivimäki, P. 2018. *Nordic Institute for Interoperability Solutions – There Is No Blockchain Technology in X-Road*. https://www.niis.org/blog/2018/4/26/there-is-no-blockchain-technology-in-the-x-road?ref=hackernoon.com (accessed 13 May 2022).

Magrath, M. 2022. *New US Digital Identity Legislation Promises More Secure Verification*. https://www.csoonline.com/article/3575423/new-us-digital-identity-legislation-promises-more-secure-verification.html (accessed 13 May 2022).

Mobile Ecosystem Forum (MEF). 2021. *Italy Demonstrates Success in Mass Adoption of a Digital Identity Scheme with SPID*. https://mobileecosystemforum.com/2021/09/07/italy-demonstrates-success-in-mass-adoption-of-a-digital-identity-scheme-with-spid/ (accessed 13 May 2022).

My.Gov.Sa. 2022a. *Digital Transformation – Digital Identity*. https://www.my.gov.sa/wps/portal/snp/aboutksa/digitaltransformation (accessed 13 May 2022).

My.Gov.Sa. 2022b. *Issuing a National Identity Card*. https://www.my.gov.sa/wps/portal/snp/servicesDirectory/servicedetails/9511 (accessed 13 May 2022).

Namirial. 2021. *The Current Situation of the Adoption of the SPID Identity in Italy*. https://www.namirial.com/en/digital-identity-state-of-play-italy-end-of-2021/ (accessed 13 May 2022).

National People's Congress of the People's Republic of China. 2022. *Personal Information Protection Law of the People's Republic of China*. http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (accessed 10 June 2022.

NFCW. 2022. *China to Roll Out Digital ID Cards Nationwide*. https://www.nfcw.com/2022/03/16/376546/china-to-roll-out-digital-id-cards-nationwide/ (accessed 13 May 2022).

Norberg, H C., E. Ganne, and N. Hewett. 2020. *Super Charging Trade With a Trusted Global Digital Identity System*. https://www.unescap.org/sites/default/files/86%20Final-Team%20Hanna%20Norberg-Sweden.pdf (accessed 13 May 2022).

Nubian Rights Forum & 2 Others v Attorney General & 6 Others (2020). Accessible at https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html (accessed 13 May 2022).

Penzenstadler, N. 2022. *How Scammers Siphoned $36B in Fraudulent Unemployment Payments from US*. https://www.usatoday.com/in-depth/news/investigations/2020/12/30/unemployment-fraud-how-international-scammers-took-36-b-us/3960263001/ (accessed 10 June 2022).

Privacy International. 2017. *Aadhaar Security Fail*. https://privacyinternational.org/aadhaarsecurityfails (accessed 13 May 2022).

Privacy International. 2022a. *Data Protection Impact Assessments and ID Systems: The 2021 Kenyan Ruling on Huduma Namba*. https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma (accessed 13 May 2022).

———. 2022b *Digital National ID Systems: Ways, Shapes and Forms*. https://privacyinternational.org/long-read/4656/digital-national-id-systems-ways-shapes-and-forms (accessed 13 May 2022).

———. 2022c. *ID Systems Analysed: E-Estonia*. https://privacyinternational.org/case-study/4737/id-systems-analysed-e-estonia (accessed 13 May 2022).

———. 2022d. *Kenyan Court Ruling on Huduma Namba Identity System: The Good, the Bad and the Lessons*. https://privacyinternational.org/long-read/3373/kenyan-court-ruling-huduma-namba-identity-system-good-bad-and-lessons (accessed 13 May 2022).

———. 2022e. *Understanding Identity Systems Part 2: Discrimination and Identity*. https://www.privacyinternational.org/explainer/2670/understanding-identity-systems-part-2-discrimination-and-identity (accessed 13 May 2022).

———. 2022f. *Understanding Identity Systems Part 3: The Risks of ID*. https://www.privacyinternational.org/explainer/2672/understanding-identity-systems-part-3-risks-id (accessed 13 May 2022).

———. 2022g. *Why the Huduma Namba Ruling Matters for the Future of Digital ID, and Not Just in Kenya*. https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya (accessed 16 May 2022).

Research ICT Africa and CIS. 2021. *Digital Identity in Kenya: Case Study Conducted as Part of a Ten-Country Exploration of Socio-digital ID Systems in Parts of Africa*. https://researchictafrica.net/wp/wp-content/uploads/2021/11/Kenya_1.11.21.pdf (accessed 13 May 2022).

Salyanty, A., A. Aadil, R. Febrianti, R. Kapoor, and S. Sampath. 2020. *KYC Practices in Indonesia and the Opportunity for Implementing e-KYC to Accelerate Financial Inclusion*. https://www.microsave.net/wp-content/uploads/2021/01/PB-24_-KYC-practices-in-Indonesia.pdf (accessed 13 May 2022).

Saudi Gazette. 2021. *Saudi Citizen's Digital ID Launched*. https://saudigazette.com.sa/article/602160 (accessed 13 May 2022).

SMEX. 2021. *The Digital ID Landscape in the GCC: A Mapping of Programs, Regulations and Human Rights Risks*. https://smex.org/wp-content/uploads/2021/12/The-Digital-ID-Landscape-In-the-GCC-1.pdf (accessed 13 May 2022).

SPID. 2022a. Frequently Asked Questions. https://wwwspid.gov.it/en/frequently-asked-questions/#what-is-spid (accessed 13 May 2022).

———. 2022b. *SPID – Sistema Pubblico Di Identità Digitale*. https://www.spid.gov.it/?msclkid=dc3a740ec62011ec9c86b288cd52ee0f (accessed 13 May 2022).

Ssa.Gov. 2022. *Consent Based Social Security Number Verification (CBSV) Service*. https://www.ssa.gov/cbsv/ (accessed 13 May 2022).

Stone, M. 2021 *How Estonia Created Trust in Its Digital-Forward Government*. https://securityintelligence.com/articles/estonia-trust-digital-government/ (accessed 13 May 2022).

Totapally, S., P. Sonderegger, P. Rao, J. Gosselt and G. Gupta. 2019. *State of Aadhaar: A People's Perspective*. https://stateofaadhaar.in/assets/download/SoA_2019_Report_web.pdf?utm_source=download_report&utm_medium=button_dr_2019 (accessed 10 June 2022).

Trulioo. 2019. *100,000 Years of Identity Verification: An Infographic History*. https://www.trulioo.com/blog/infographic-the-history-of-id-verification (accessed 13 May 2022).

Unique Identification Authority of India (UIDAI). 2012. *Role of Biometric Technology in Aadhaar Enrollment*. https://external.privacyinternational.org/s/RX8SemLJMtrK3LE (accessed 16 May 2022.

World Bank. 2021. *Principles on Identification for Sustainable Development: Toward the Digital Age*. https://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf (accessed 16 May 2022).

World Economic Forum (WEF). 2022. *This Kenyan Ruling on Digital ID May Have Global Impact*. https://www.weforum.org/agenda/2022/03/kenyan-supreme-court-digital-id-online-privacy/ (accessed 13 May 2022).

Zheng, W. 2022. China Plans Digital Version of National Identification Card Later this Year. *South China Morning Post*. 12 March. https://www.scmp.com/news/china/politics/article/3170214/china-plans-digital-version-national-identification-card-later (accessed 10 June 2022).

**Asian Development Bank Institute**

ADBI, located in Tokyo, is the think tank of the Asian Development Bank (ADB). Its mission is to identify effective development strategies and improve development management in ADB's developing member countries.

ADBI Policy Briefs are based on events organized or co-organized by ADBI. The series is designed to provide concise, nontechnical accounts of policy issues of topical interest, with a view to facilitating informed debate.



**Asian Development Bank Institute**
Kasumigaseki Building 8F
3-2-5 Kasumigaseki, Chiyoda-ku
Tokyo 100-6008
Japan
Tel: +813 3593 5500
www.adbi.org