Chapter 4
Digital Identity

Digital Identity

Key points

- Digital identity is a keystone issue in helping an additional 1.1 billion people—mostly in Africa and Asia—to access financial services.
- Analogue, paper-based identity systems are siloed and inflexible, exacerbating financial exclusion. Digital identity systems remedy many of these effects.
- Experiments with digital identity are being conducted across the Commonwealth, with an emphasis on federated (versus centralised) approaches.
- Public consultation prior to introducing a new identity system is key to its success. This allows users to make valuable comment on the system's design, and it builds their trust and confidence in the system, which can help to drive its adoption.

4.1 Introduction

The World Bank estimates that there are more than 1.1 billion people globally who are unable to prove their identity with official documentation. As a result, they lack access to financial services, health care, education and social services. Most of these people are in Africa and Asia.[1] Global consulting firm McKinsey & Co. estimates that another 1 billion people have formal identity documentation (often referred to simply as ID) but cannot use it on digital channels, locking them out of the digital economy, while 45 per cent of women over the age of 15 in low-income countries lack ID compared to 30 per cent of men.[2]

The World Bank has highlighted the introduction of robust, inclusive and responsible digital identity systems as a priority action with the potential to progress many of the United Nations Sustainable Development Goals (SDGs), including aspects such as social protection, the empowerment of women and girls, financial inclusion, governance, health care, digital development and humanitarian assistance.[3]

> Digital identity systems have the potential to allow more people to access basic services, including financial services, fuelling economic growth and reducing human rights abuses.

Global challenges such as the refugee crisis in Latin America, Europe and other regions, as well as the 3.5 billion people who are underbanked or unbanked because financial services institutions cannot verify their identity or assess their credit profile (an attribute of their identity), highlight the need for a viable identity solution.[4]

These challenges inevitably result in the exploitation of those without legal ID and the economic exclusion of those without legal ID. Moreover, the value that people add to an economy is lost when they have no ID or have ID but cannot use it on digital channels, giving the government no way of tracking their contributions.

Digital identity systems have the potential to address these wide-reaching implications, allowing more people to access basic services, including financial services, fuelling economic growth and reducing human rights abuses. McKinsey & Co. estimates that digital or electronic ID has the potential to add economic value of at least 3 per cent and potentially as much as 13 per cent of gross domestic product (GDP) by 2030.[5]

4.2 Context

In its simplest form, ID is supporting evidence that an individual is who they say they are. It has been suggested that the very first government-issued form of ID were the letters with which ancient Persian king Artaxerxes guaranteed prophet Nehemiah safe passage to Jerusalem in 450BCE. Later, in 1414, King Henry V granted 'safe conduct' documents in what is believed to be the first form of 'passport'.[6]

As the passport has developed, it has continued—even in its most advanced form—to centre on evidencing identity in face-to-face transactions. Moreover, it is common knowledge that a passport and other similar forms of ID can be, at the very least, inaccurate; at worst, it might be forged. There are also limitations to any form of ID that relies on an address as evidence of identity—especially in many developing economies and rural areas, where people with the same or similar names may live at the same address.

In the modern electronic era, it is becoming increasingly difficult to prove that we are who we say we are, even if we have ID. While some simple transactions do not require the parties to verify each other's identities, if a person is to participate in modern society—and especially if they are to access financial services—they need a verifiable form of identity.

4.2.1 The Basic Functions of an Identity System

The implications of today's legacy ID systems are wide-ranging, with differing impacts on those who have no ID and those who have ID that they cannot use digitally.

As Figure 4.1 outlines, an ID is one component of a system that:

- identifies an individual;
- authenticates that identity; and
- grants (or withholds) access depending on whether that individual is authorised or eligible to participate in the activity they are requesting.[7]

4.2.2 The Flaws in Legacy Identity Systems

It is evident that current identity systems are broadly inefficient and often ineffective. The design of legacy systems is:

- document-based, making them cumbersome, as well as prone to human error and exploitation;

Figure 4.1 The basic roles of an ID system.

Who are you?	Are you who you claim to be?	Are you authorised or eligible?
1	2	3
Identification	*Authentication*	*Authorisation*
Establishing a person's identity by gathering and checking relevant identity information	Checking that a person is who they claim to be based on evidence of one or more personal details	Checking specific attributes to confirm whether or not a person is authorised or eligible to participate

Source: Adapted from World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

- siloed, storing identity information discretely; and
- inflexible, with current forms of identity codified in documents that cannot easily be adapted to meet modern transaction requirements.[8]

Any new identity system, digital or otherwise, should address these shortfalls and their implications.

More specifically, inefficient and ineffective legacy systems leave behind those who **have no formal ID**, with profound impacts, including:

- the economic exclusion of individuals and (sometimes large) groups of people;
- the exclusion of individuals and groups of people from basic services such as health care and social services;
- the exclusion of refugees who often cannot relocate without formal ID;
- constraints on economic development when financial services and other businesses cannot deliver to individuals and populations;
- compromised national safety and security when nation-states are unable to identity and manage the people crossing their borders; and
- issues of regulatory compliance for financial services and other businesses that are required to adhere to anti-money-laundering (AML) or know your customer (KYC) rules.

Even those who **have an ID but cannot use it digitally** experience some of these impacts, including:

- exclusion from digital services when those services fail to recognise formal ID;
- exclusion from financial services where their ID does not meet AML/KYC requirements, which also strips the economy of the value that individual would otherwise add; and
- the costs of compromised or forged ID, which represent both personal

and financial risks for individuals and can render a cost to financial services institutions and public services should, for example, false ID be used to claim social services benefits.

4.3 Description

4.3.1 What is Identity in the Modern Era?

We can conceive of identity as a series of attributes—physical, legal, electronic and behavioural—that combine to form a unique picture of an individual.

- **Physical attributes** are the features that identify an individual uniquely and are harder to forge or manipulate than others. They include a person's DNA, as well as *physical biometrics* such as fingerprints and facial features. Recent technological advances based on facial recognition and scanning fingerprints have, however, proved to be easily hacked.

- **Legal attributes** are those associated with the 'traditional' forms of ID that are widely used globally, such as a driver's licence or passport. Increasingly, these forms of ID are now supplanted or augmented by physical biometrics (*see above*).

- **Electronic attributes** are those that relate to the increasing amount of time individuals are spending online and on their mobile or smartphones. They include details such as a person's email address, social media accounts, online actions and Internet Protocol (IP) address. Increasingly, advertisers and other parties are using individuals' IP addresses to track and trace their online actions, which data the advertisers then commercialise.

- Using **behavioural attributes** as a form of identification is a recent technology and it has been shown to be a unique, reliable means of identifying an individual. This type of data includes details such as locations visited and spending patterns, and using this data as part of identity is part of a growing field known as *behavioural biometrics*.[9]

It is now widely accepted that legal attributes and traditional forms of ID are flawed and are open to abuse. While each of the above attributes can be used individually to identify a person, they are more powerful and reliable when used in combination—and advances in technology have allowed actors to explore their potential in relation to a new form of *digital* identity.

4.3.2 Digital Identity

A digital identity can be defined as a set of digital records that verify that an individual is who they say they are and allow them to engage in transactions in the modern—digital—world.[10] McKinsey & Co. benchmarks a 'good' digital identity as being:

- verifiable to a high degree of assurance;

- unique; and

- established with an individual's consent.

Digital identity systems have been trialled and implemented in, for example, India, Estonia, the Nordic regions, Singapore and Canada. India created the Aadhaar project in 2009, which now covers an estimated 89 per cent of its population, while the others have also all deployed formats of an electronic identity—or e-ID—system (*see later in this chapter*).

4.3.3 Digital Identity Technologies

The proliferation of mobile phone technology is one of the most significant contributory factors in the development of digital identity. Among the data that our mobile phones gather is **biometric identity** data. Biometric identity systems use facial recognition, fingerprints, heartbeats, speech patterns, walking patterns and hand movements to build a picture of an individual's unique biometric attributes with which they can be identified.[11]

The volume of data that is collected, available and shared through our mobile phones is vast, and the value of that data is growing—to such an extent that the World Economic Forum (WEF) considers personal data is be an emerging asset class.[12] While traditional identity attributes are commonly gathered in large databases that are vulnerable to hackers, as this sensitive personal data accumulates and new models aim to monetise identity data for the benefit, rather than the detriment, of individuals, new technologies are solving new problems. **Encryption** secures that identity data, for example, and **tokenisation** organises the attributes so that they can be managed and monetised more readily.[13]

We encrypt (encode) data by inputting it—together with another parameter (or 'key')—into an encryption algorithm (or 'cipher'). There are two basic methods of encryption for securing data transmission:

- *symmetric encryption*, whereby a single key—a shared secret—is used to both encrypt (encode) and decrypt (decode) information; and
- *asymmetric encryption* (also known as public key encryption), whereby a pair of related keys are used—one to encrypt the data and the other to decrypt it.[14]

In that context and in light of data protection principles, **self-sovereign ID** is a model that centres the user in the administration of their identity. Historically, an oligopolistic, corporate entity might have expected to hold a user's personal data in a central database or data repository; now, a decentralised identity system will give the user absolute control over their own identity data and the benefits to the consumer are numerous. Not only is an individual granted more insight into who is using or reviewing their personal information, but also they can exercise control over the financial or health data that allows them to access better financial or health-care services, and they can even take advantage of the 'right to be forgotten' enshrined in the General Data Protection Regulation (GDPR) in the European Union (EU).[15]

> The volume of data that is collected, available and shared through our mobile phones is vast. The value of that data is growing to such an extent that the World Economic Forum (WEF) considers personal data to be an emerging asset class.

4.3.4 Introducing Digital Identity Systems

While it is clear that digital identity has the potential to remedy gaps in current legacy systems, digital identity systems are not without their risks. Such risks can include, among others:

- stakeholders rejecting the technology because they do not trust it and they have been consulted only inadequately on its introduction;
- the technology being ineffective because of inadequate planning;
- insufficient technical support or public education to drive widespread adoption and facilitate efficient use;
- unsustainable operations because of inefficient systems design and/or high costs; and
- policy changes at a governmental level.

To mitigate these risks, large-scale digital identity projects may take one of three main approaches to governance.

- Centralised approach Identity is handled by a single (usually public) entity. This approach allows for streamlined decision-making and implementation, as well as high data aggregation capability, but positioning the system with only one entity has implications for risk, liability and cost. Examples of this type of approach are the digital ID programmes launched by India and Estonia.
- Federated approach In this model, a few entities establish a formal digital identity network. This approach spreads the cost and mitigates the potential for abuse, but it does introduce the need for co-ordinated decision-making, which adds complexity. Examples of this approach include SecureKey Concierge in Canada and NemID in Denmark (both led by financial institutions), gov.uk's Verify (launched by the public sector), and Sweden's BankId (a public–private partnership, or PPP).
- Decentralised approach This type of entity would be part of an open—potentially blockchain (see Chapter 3)—network with no institutional owners. The benefits of this approach include centring the user's control over the data and a minimised risk of abuse or manipulation by a central managing authority. However, such models remain in the early stages and have not yet been tested at scale, while there are security challenges inherent to such a system. Examples include TUPAS in Finland (a private sector solution) and Solid, launched by Tim Berners-Lee in 2018.[16]

With each of these approaches, the more centralised the approach, the more cost-effective and easy it is to implement, but the higher the degree of trust that the data-holding party must command.[17]

4.4 Key Considerations for Future Development

In looking to the future of digital identity and digital identity policy, some of the issues include stakeholder consultation and regulation.

4.4.1 Stakeholder Consultation

Governments must take the needs of all stakeholders into account when developing a digital identity policy. Public consultation at the very outset of the project will be key to building trust and buy-in, which user input on the system's design can help to drive its adoption and improve the overall success of the project.

Among the parties with which government must consult are citizens, private sector stakeholders, civil society representatives and stakeholders within government itself.

4.4.2 Regulation

Given that a range of different attributes constitutes digital identity, when developing a digital identity policy it is also imperative to consider how that personal information is managed and how much control the user is given of that information. The GDPR is the high-water mark of data protection and privacy regulation, and policies covering data protection and privacy should be measured against it.[18]

A useful tool in policy-making around digital identity is privacy by design (PBD), which sets out seven foundational principles for user privacy.[19] Any public or private actor making policy or building digital identity systems should:

1. be proactive not reactive;
2. lead with privacy;
3. embed privacy;
4. retain full functionality;
5. ensure end-to-end security;
6. maintain visibility and transparency; and
7. respect user privacy.

In relation to the fifth principle, cybersecurity (see Chapter 6) is a key factor in developing a digital identity policy and system, and should underpin any new (and indeed legacy) security and legal frameworks.[20] Encryption is a critical aspect of cybersecurity in any system containing sensitive information.[21] We should assume that any system storing personal information will be subject to cyber attack and encrypt that data accordingly.

More broadly, legislation and regulation—the legal framework at both national and supranational levels—is likely to prescribe behaviours relating to digital identity that will include, for example, rules of issuance and AML/KYC requirements in financial services. Remaining up to date with these and ensuring that any digital identity policies and systems are compliant will be crucial to their success.[22]

In the regulatory context and others, when it comes to designing any digital identity policy and system, interoperability—that is, how digital identity and aspects of digital identity will be generated, managed and combined—is important. One example of an effort to increase interoperability is the EU's eIDAS Regulation, which ensures that people and businesses can use their e-IDs to access public services across borders.[23]

4.4.3 The Guiding Principles for Robust Digital Identity Policies and Systems

The WEF outlines the following guiding principles to inform decision-making when developing robust and value-adding systems and, in this case, policies.

- Social good The system should be available to all users and designed to deliver maximum benefit to the widest possible range of stakeholders. It should be non-discriminatory and inclusive.
- Privacy-enhancing User information must be exposed to and shared with only the *right* entities under the *right* circumstances.
- User-centric Users must have control over their own information and be able to determine who holds and accesses it.

- **Viable and sustainable** The system must be economically sustainable and resilient to shifting political priorities.
- **Open and flexible** The system must be built on open and flexible standards to allow scaling and development, and those standards and guidelines must be transparent to stakeholders.[24]

In all of this, one thing is very clear: capturing the potential value of digital identity will demand careful system design and deliberate government policies if we are to mitigate the risks.[25]

Endnotes

1 World Bank (2017). '1.1 Billion "Invisible" People without ID Are Priority for New High Level Advisory Council on Identification for Development'. Press release, 12 October [online]. Retrieved from: www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development

2 McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx

3 World Bank (2017). '1.1 Billion "Invisible" People without ID Are Priority for New High Level Advisory Council on Identification for Development'. Press release, 12 October [online]. Retrieved from: www.worldbank.org/en/news/press-release/2017/10/12/11-billion-invisible-people-without-id-are-priority-for-new-high-level-advisory-council-on-identification-for-development

4 Chamber of Digital Commerce (2017). *Blockchain and Financial Inclusion* [online]. Retrieved from: https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf

5 White O *et al.* (2019). 'Digital Identification: A Key to Inclusive Growth'. *McKinsey.com*, 1 April [online]. Retrieved from: www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-identification-a-key-to-inclusive-growth

6 Benedictus L (2006). 'A Brief History of the Passport'. *The Guardian*, 17 November [online]. Retrieved from: www.theguardian.com/travel/2006/nov/17/travelnews

7 World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

8 World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

9 Schukai R, Chadwick S, Baker T (2017). 'Who Are You? Defining Digital Identity and Authentication Technologies'. *Thomson Reuters*, 28 June [online]. Retrieved from: https://blogs.thomsonreuters.com/answerson/digital-identity-authentication-technologies/

10 World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

11 Glaser A (2016). 'Biometrics Are Coming, Along With Serious Security Concerns'. *Wired.com*, 9 March [online]. Retrieved from: www.wired.com/2016/03/biometrics-coming-along-serious-security-concerns/

12 World Economic Forum (2011). *Personal Data: The Emergence of a New Asset Class* [online]. Retrieved from: www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

13 World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

14 *Ibid.*

15 Allen C (2016). 'The Path to Self-sovereign Identity'. *Coindesk*, 27 April [online]. Retrieved from: www.coindesk.com/path-self-sovereign-identity; Regulation (EU) 2016/679

of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, 4 May 2016, OJ L 119/1.

[16] McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx

[17] *Ibid.*

[18] European Commission (2020). 'Complete Guide to GDPR Compliance' [online]. Retrieved from: https://gdpr.eu/

[19] Deloitte, Ryerson University (2016). *Privacy by Design: Setting a New Standard for Privacy Certification* [online]. Retrieved from: www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-ers-privacy-by-design-brochure.PDF; Cavoukian A (2011). 'Privacy by Design: The 7 Foundational Principles'. *Internet Architecture Board*, March [online]. Retrieved from: https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

[20] GSMA (2016). 'Digital Identity: Regulatory Trends and the Role of Mobile'. 3 November [online]. Retrieved from: www.gsma.com/mobilefordevelopment/programme/digital-identity/digital-identity-regulatory-trends-and-the-role-of-mobile/

[21] World Bank (2019). *ID4D Practitioner's Guide* [online]. Retrieved from: http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf

[22] GSMA (2016). *Regulatory and Policy Trends Impacting Digital Identity and the Role of Mobile: Considerations for Emerging Markets* [online]. Retrieved from: www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/10/Regulatory-and-policy-trends-impacting-Digital-Identity-and-the-role-of-mobile.pdf

[23] Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, 9 September 2015, OJ L 235/1.

[24] World Economic Forum (2016). *A Blueprint for Digital Identity* [online]. Retrieved from: www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

[25] McKinsey & Co. (2019). *Digital Identification: A Key to Inclusive Growth* [online]. Retrieved from: www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Innovation/The%20value%20of%20digital%20ID%20for%20the%20global%20economy%20and%20society/MGI-Digital-identification-A-key-to-inclusive-growth.ashx