Digital Identity Toolkit

Section 1: Toolkit introduction

May 2023

What is this Toolkit?

Digital identity is a relatively new but rapidly evolving sector that can and will affect many aspects of our everyday lives.

Digital identities verify and authenticate someone's identity. They can then be used to access a wide range of services and opportunities, from health and education services, voting and travelling, through to online shopping and dating. Governments and the private sector are developing and implementing digital identity solutions, and they're likely to become increasingly common in the future.

While there is already a lot of information on this topic, much of it is in lengthy, technical reports and hasn't been collated into a simple format that non-technical people can understand. We hope this Toolkit can help close that gap.

This Toolkit has been designed to help you find everything you need to know about digital identity. Before producing it, we spoke with individuals and non-profits around the world to get a sense of what they'd like to know about digital identities.

The audience for this Toolkit is members of the public, non-profits, entrepreneurs, developers, journalists and academics who want to learn more about digital identity and how digital identities might be relevant to them in their lives or work.

We hope you find this Toolkit helpful and welcome your feedback about how it could be improved.

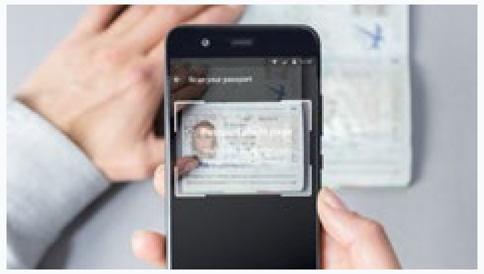
What it contains

This Introduction provides an overview of the topics covered in the subsequent sections of this Toolkit. We hope it will give you a good sense of what digital identity is all about. Feel free to download sections 2 to 7 for more detailed information on each of these topics.

The Toolkit is divided into 7 sections:

Section 1: Toolkit introduction

Section 2: Identity basics



Section 3: Digital identities explained

Section 4: Case studies

Section 5: Digital identity solutions

Section 6: Data privacy and security

Section 7: Reports and further reading

Section 2:
Identity basics

Identification is a way of recognising someone as a unique individual, and can be used to verify that somebody is who they say they are.

You need an identity, or some way of proving who you are, to access a whole range of opportunities in the modern world. Examples include: accessing public services, such as healthcare and education; receiving public support, such as pensions, unemployment benefits and loans; travelling to another country; voting; buying or selling land; and accessing commercial opportunities, such as opening a bank account, buying a mobile phone or SIM card, employment in the formal sector or shopping online.

Identity really matters. Despite being recognised as a human right, an estimated 1.1 billion people globally still lack an official ID. Hundreds of millions don't even have a birth certificate. Poor, rural and marginalised populations are the most affected. Since they are unable to access some of the critical services and opportunities outlined earlier, they risk becoming even more vulnerable. Those without identification are also at risk of becoming stateless, which leaves them legally and politically invisible and destined to a life of poverty.

People have needed to identify themselves throughout human history. At first, they relied on physical features such as birthmarks or tattoos. Later, people began to rely on formal documentation, such as passports, driving licences and birth certificates.

In modern times, paper-based systems are being replaced by digital identities, which are more secure and trustworthy, can be used easily online, can't get lost, and enable users to access a whole suite of services in one go.

Section 3: Digital identities explained

Digital identity is a way of digitally verifying that somebody is who they say they are (normally online) so that they can access services from both the government (for example, healthcare, education, grants) and the private sector (for example, banking and e-commerce).

The most trustworthy type of digital identity is called a **verified** digital identity. It can include a number of different 'attributes' depending on what the digital identity will be used for, and could include one or more of the following:

- Your email address
- Headshots
- Usernames and passwords
- Biometric information (based on your fingerprints, for example)
- Your full name, nationality or date of birth

Digital identities can be set up in different ways. Governments or private companies can set up identities that you can use in different places to prove who you are or that you are entitled to a product or service. Some companies or services may have their own identity procedures, meaning you identify or authenticate yourself each time to each organisation using their identity method (such as using your fingerprint to open a banking app on your phone).

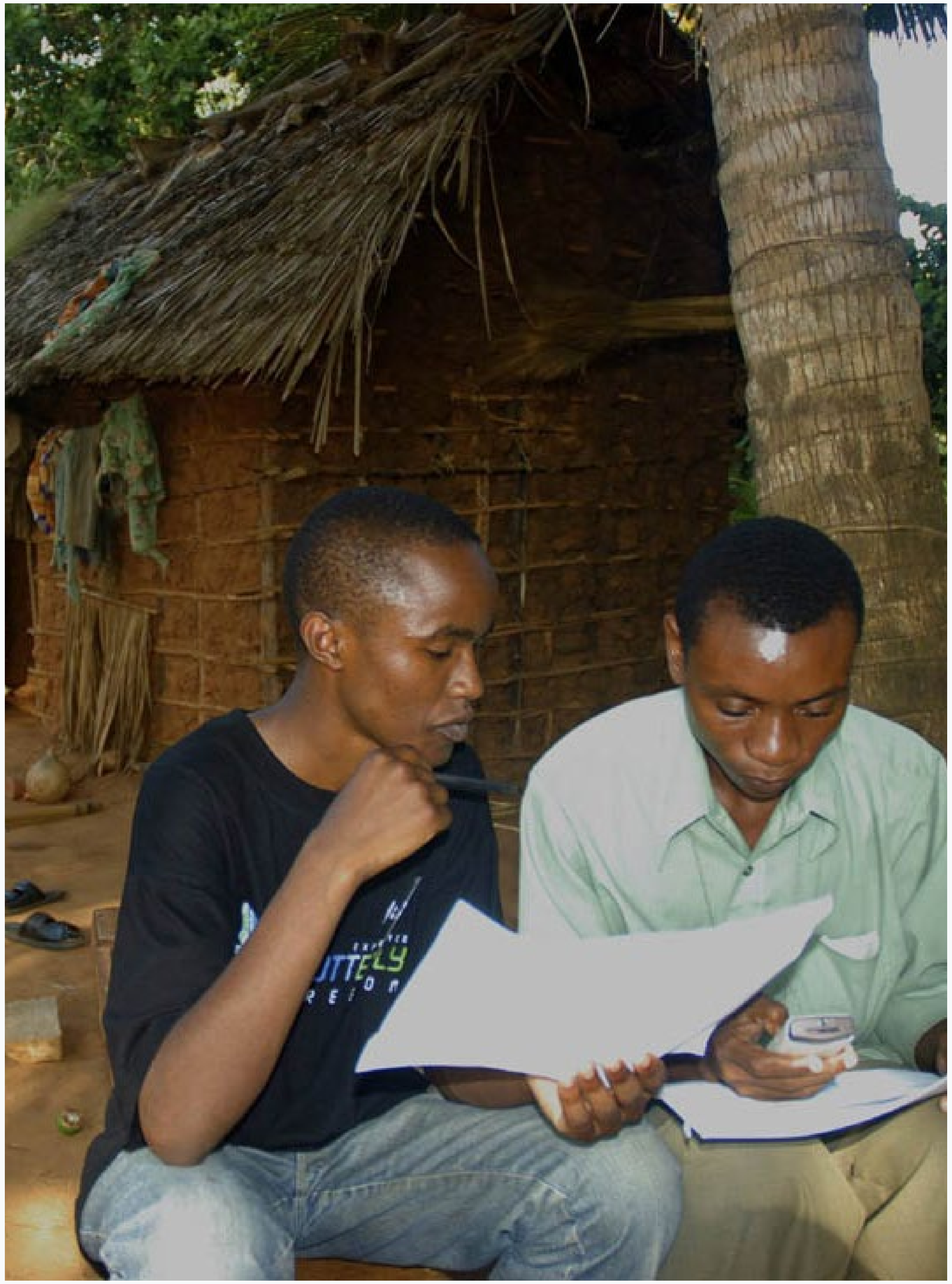
With some digital identity solutions, you can choose which attributes you want to include and can then decide which ones you want to share. This would depend on what you want to use that digital identity for. For example you may just need to share your date of birth to buy alcohol. Your identity is verified using documents or other data, such as fingerprints, which can confirm that you are who you say you are. This Toolkit mainly focuses on this type of verified identity. Other digital identity solutions require specific information and your choices may be limited to, for example, which document you use to set up the identity. For government-issued identities, the government usually decides what information is required (such as information from your passport).

Unverified digital identities also exist, and they are created by signing up to certain websites, such as Facebook and Amazon. Through using them, your preferences are recorded (your likes on Facebook, for example) and this creates a digital footprint, which becomes unique to you as an individual. This information is sometimes considered sufficient proof that you are who you say you are and can be used to access other websites and services (for instance, you can use your Facebook login to sign on to other websites). However, since it is possible to provide a false name and other information when signing up, these unverified digital identities can't be used to access public services, such as healthcare, and private services, such as banking. They're just not reliable enough.

There is a great deal of international interest in digital identity. It has been prioritised in the United Nations' Sustainable Development Goals (SDG target 16.9), and governments across the world, particularly in developing countries, are driving adoption. National digital identities based on biometric data have been introduced in India and Pakistan and are being used to help citizens access a whole range of public and private services.

Digital identity also has the potential to protect the vulnerable, including the estimated 1.1 billion people globally who still lack an official ID. It is hoped that digital identities will enable seamless global transactions across borders, help to prevent digital fraud, lower the costs and increase the efficiency of delivering services. They have the potential to strengthen democracies by enabling digital voting (thus reducing voter fraud) and can be used to provide more personalised services to individuals. Adopting secure, verifiable digital identities has the potential to open up new markets and grow economies by billions.

Without a digital identity, people are at risk of being unable to access critical public and commercial services, including purchasing property, owning land, buying a car, being able to vote, and reducing the risk of becoming homeless or stateless. These challenges disproportionately affect poor and marginalised communities, further increasing their vulnerability.



Section 4: Case studies

Governments, charities/NGOs and the private sector all use digital identities. Below are a few examples from different sectors.

Accessing government services

Governments across the world are implementing digital identity solutions that help people access public and, in some instances, private services. India's Aadhaar model helps to facilitate inclusion and deliver government services to citizens, while e-Estonia is renowned as the most highly-developed national ID card system in the world covering over 90% of the population. It allows citizens to access any public digital service, reduces bureaucracy and speeds up the process of many daily tasks. It can be used for banking, signing documents, obtaining digital medical prescriptions and for business operations.

Public and private sector national identity use

India has the world's largest national digital identity system. Known as Aadhaar, it was set up and is run by the Indian government. It has over 1.2 billion users and relies on biometric data for validation. Citizens can use it to access government services, and financial providers can use it for due diligence. Aadhaar can be used to open a bank account, file tax returns, receive a pension or receive other government subsidies.

Digital identities have also been used to improve government administration. In Japan, a cloud-based system enables national and local public agencies to seamlessly track and share information.

In Singapore, the Moments of Life initiative bundles government services and information. It uses data to anticipate citizens' specific needs as they reach key life moments, such as marriage or the birth of a child.

Addressing social challenges

Digital identity can also address a whole range of social challenges. Many countries are now registering births digitally. This is a critical type of digital identification as birth registration is often the gateway to accessing services, such as health and education, throughout life. iCivil in Burkina Faso is an example of this.

In India, Aadhaar is used in the education system to access student scholarships, online courses and track attendance. In Pakistan, computerised national identity cards are used for cash transfers, voting rights and opening bank accounts.

Digital identification is also improving health outcomes globally. Botswana uses national digital identification numbers to track adherence and adverse reactions to antiretroviral therapy in patients with HIV across the country's decentralised health facilities. Thailand has a digitised national population register and digital personal identification numbers for the successful implementation of a universal coverage scheme, guaranteeing subsidised healthcare to all citizens. It is also used to track vaccinations, produce vital statistics that guide public health policy and to monitor health system performance.

Nigeria and Estonia have digitised agricultural subsidies, and in Malaysia land registration is digitised and uses fingerprint readers to reduce fraud. Farmers also have unique digital profiles which can be used to track market attendance and receive agricultural extension services. Uruguay has implemented a digital livestock traceability system for cattle.

Uganda has a web-based refugee information management system to issue ID cards to refugees so they can access special entitlements, including discounted education and healthcare. Jordan, Lebanon and Egypt use digital refugee assistance information systems to monitor and coordinate humanitarian aid. This is an inter-agency tool for tracking assistance, referrals and assessment information.

Private sector case studies

The private sector is also building solutions to give customers safe and efficient access to public and financial services. Examples include NemID in Denmark, BankID in Norway and Sweden, and TUPAS in Finland. In the Caribbean, Juvo's Flow Lend solution enables Cable & Wireless prepaid mobile customers to establish a financial (functional) identity, which gives customers access to airtime credit.

In the retail sector, Komplett, one of Europe's biggest e-trade companies, uses the Signicat digital identity platform for rapid online payments, and in China customers can pay for their online shopping at Alibaba or at KFC restaurants by scanning their fingerprints or through facial recognition (staring at a camera).

The United Arab Emirates has released a digital smart wallet app to replace paper-based travel identity documents, such as passports, and the government is creating a 'biometric border' which will use facial recognition scanners to verify a traveller's identity.

Financial institutions and regulators also use digital identities to undertake due diligence. For example, the Global Legal Entity Identifier Foundation is working to create a standardised global view of legal entities, whilst in Spain, a consortium of banks is using a blockchain platform to create a digital identity designed to counter money laundering and boost KYC (know your customer) efforts.

Section 5: Digital identity solutions

There are many verified digital identity solutions. Section 5 of this Toolkit summarises 12 of these solutions, all of which have been launched by non-profits or national governments: 121, Aadhaar, Biometric Identity Management System (BIMS), Dignified Identities in Cash Assistance (DIGID), e-Estonia, iRespond, Last Mile Mobile Solutions (LMMS), Modular Open Source Identity Platform (MOSIP), OpenCRVS, RedRose, SCOPE and Simprints.

While not designed to be an exhaustive list, Section 5 should give you a sense of how digital identity is used, the breadth of options which exist and some insights into which may be the best for you, whether you are looking for a solution for your NGO, government department or business, or are just interested in the different approaches to digital identity.

Simprints, for example, specialise in providing digital identity solutions to healthcare providers, working with organisations including BRAC and Mercy Corps. BIMS is a biometric identity system created by the UNHCR to facilitate aid distribution for refugees, whilst e-Estonia is a national digital identification system used by Estonian citizens to access a range of government services online.

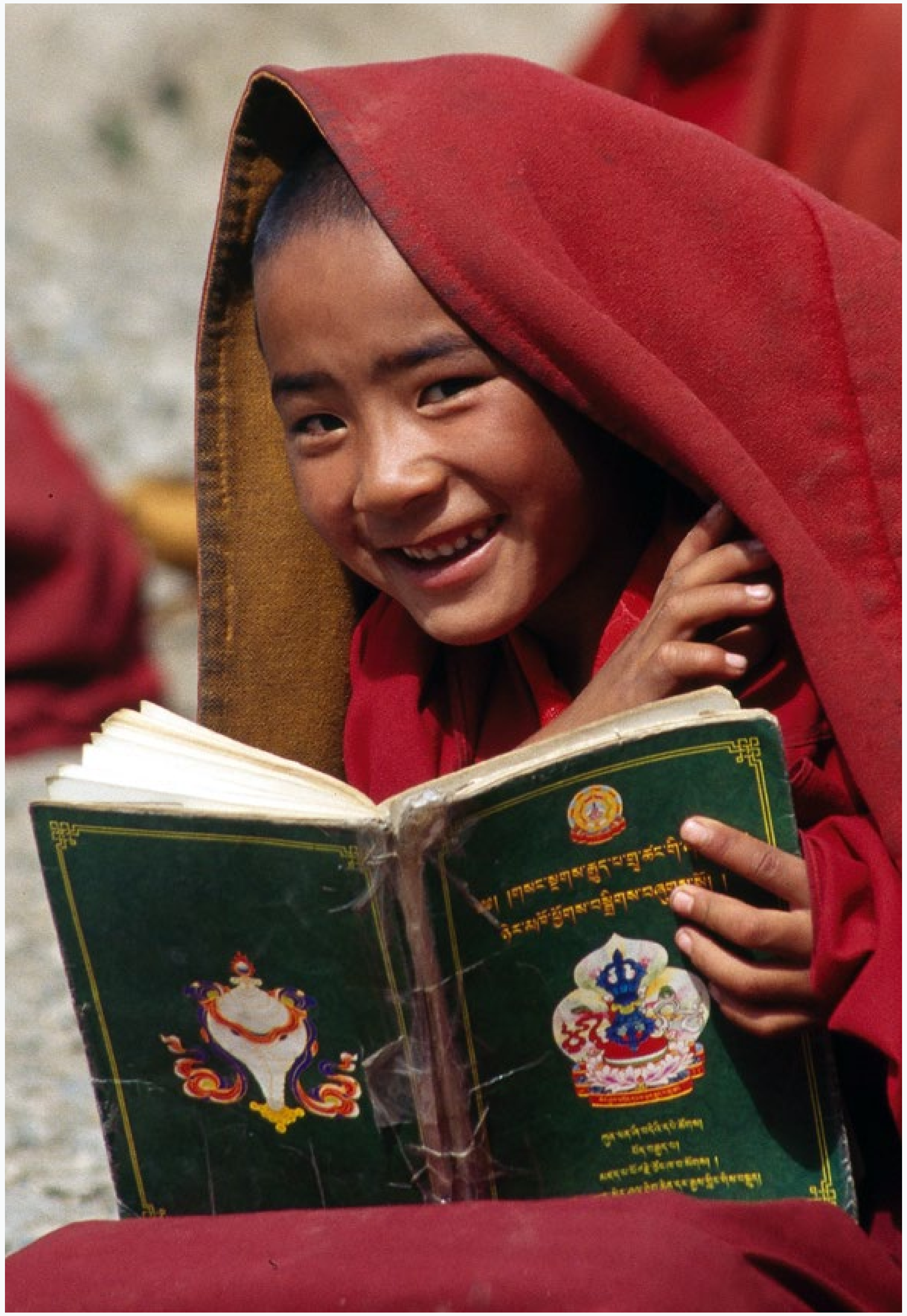
To help you better understand what each provider offers, we have broken the details down into the following sections: what the solution is, who developed it, how it works, its unique selling points, and its key uses.

Section 6: Data privacy and security

It is critical to consider both privacy and security matters as part of developing a digital identity system. Section 6 looks at the key privacy and security points that you need to factor in as you plan, develop and build a digital identity system. It has a detailed checklist of questions to help you protect your users' privacy and security at every stage, and to help you avoid falling foul of any data protection or privacy regulations, such as the EU's GDPR legislation.

Section 7: Reports and further reading

This section provides a list of reports on digital identity. Many of these are white papers from the World Bank or consultancies. They explore different types of digital identity, look at the uses of digital identity globally in different sectors and provide greater insight into digital identities as a whole. If you are looking for a more in-depth perspective on the current and future state of digital identity, these reports will provide that for you.



Glossary

Term	Meaning
AML	**Anti-money laundering** checks are carried out by regulated businesses to perform due diligence and prevent financial crime.
API	**Application Programming Interface** refers to the software that allows for communication between two computer programs, such as applications, e.g. when Yoti shares your age with an app.
Back-end system	The infrastructure and system behind the 'front-end' of the digital identity solution. **API** would be a part of back-end system design.
Biometrics	**Biometrics** relate to the physical characteristics that can be used to identify individuals. Examples include fingerprint mapping, facial recognition or iris scans.
Blockchain	A way of recording information, so that it is stored across several computers connected in a network. This makes it almost impossible to exploit the system, creating a secure technology.
Cloud Infrastructure	The collection of elements needed for cloud computing. It includes hardware, software, network resources, computing power and storage.
GDPR	**General Data Protection Regulation** is legislation set out by the EU to protect the personal information of all data subjects within the region.

Term	Meaning
IDSP	**Identity Service Providers**, sometimes referred to as identity providers, allow people to remotely verify their identity.
KYC	**Know-Your-Customer** checks form a part of due diligence, which allow institutions to verify the identity of a customer whilst doing business with them.
MFA/V	**Multi-Factor Authentication/Verification** refers to a security measure in which the user must present at least two pieces of evidence to access a particular service. Alongside a username and password, the additional verification factor is usually based on one of the following things: something you know (e.g. a password), something you have (e.g. a mobile phone), or something you are (e.g. biometric data in the form of a fingerprint).
Open Source	This is a copyright licence under which the user can amend, use and distribute software. This is particularly helpful in easily creating digital identity platforms.
PII	**Personal Identifiable Information** is any data that can reveal someone's identity, either directly or indirectly. This must be protected at all times.
RP	A **Relying Party** refers to a server allowing access to secure software.
SDG	The UN has set out 17 **Sustainable Development Goals**. SDG 16.9 aims to provide legal identity for all, including birth registration.
SDK	A **Software Development Kit** is a collection of software development tools that makes it easier to develop an application, such as one for digital identity. It may also contain a software framework.

Published by the Social Purpose Team at Yoti
www.yoti.com/social-purpose