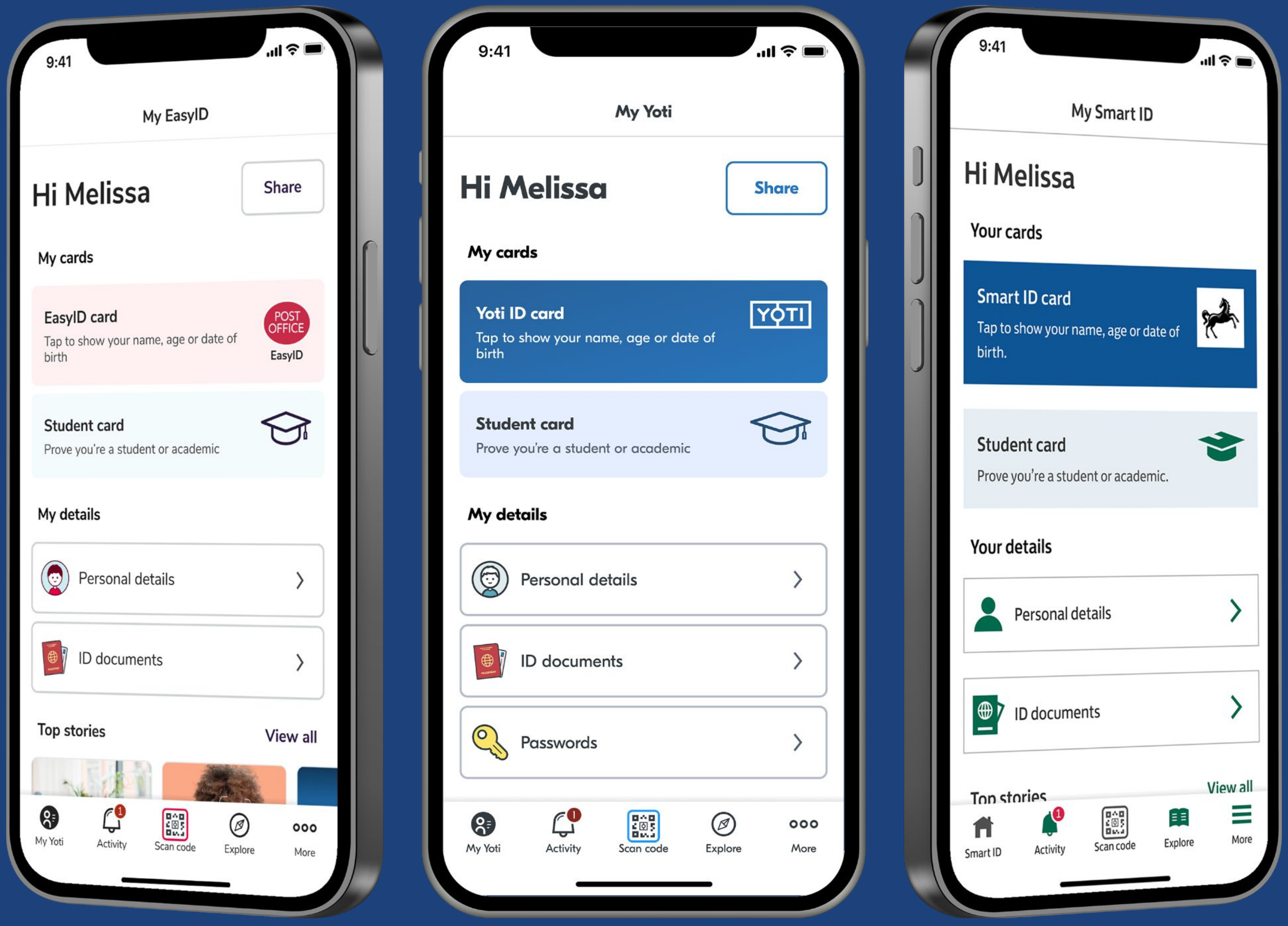
What is Digital ID?

Digital identity report series: 1

November 2024



Introduction

When we need to prove our age or identity, we are usually required to show a physical document, like a passport or driving licence. Presenting these documents allows a business to confirm that someone is who they say they are.

But the way we prove who we are is changing. Paper-based systems are being replaced by digital identities which are more secure and trustworthy, can be used easily online, and enable users to access a whole suite of services anytime, anywhere.

Digital identity is a relatively new but rapidly evolving sector that can and will affect many aspects of our everyday lives. Digital identities can be used to access a wide range of services and opportunities, from opening a bank account, renting a property and even buying age-restricted items.

Governments and the private sector are developing and implementing digital identity solutions, and they're likely to become increasingly common in the future.

In this report series, we delve into digital identity, exploring the benefits for businesses and individuals, and how it is shaping interactions and trust around the world.

What do we mean by digital identity

Digital identity can mean many things to different people, different scenarios and varying definitions within regulations.

The broadest definition would be any part of yourself, or account, that is online. It's a way of digitally verifying that somebody is who they say they are. This 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:

- Single sign on: social media account or email account that you also use to sign in to other accounts
- Email address/username and password
- Biometric information (such as fingerprint or FaceID)
- Personal information like full name, address and phone number

These are all ways you could use to both show and prove who you are, in a broad sense.

Single use identity verification

In scenarios where people need to prove who they are online (for example, when signing up for financial services) people are often asked to enter personal information into a form which can then be cross referenced to multiple data sources to ascertain if they are that person.

In scenarios where this does not give organisations enough confidence or where there is not enough data on the individual, people are asked to scan in government issued identity documents (such as passports or driving licences). They will often be asked to take an image of their face which is then matched to the document to be sure it's owned by them.

At Yoti we call this Identity Verification. It is a single use transaction that needs to be repeated by the individual every time they need to prove who they are.

What is a reusable digital ID?

Reusable digital IDs are the natural evolution of Identity Verification. When a verified identity can be securely stored, and only accessed by an individual, it gives them the ability to prove who they are in seconds.

At Yoti we believe there are two types of reusable digital identity:

1) Digital ID Wallets: This is where an individual verifies themselves once with a free digital ID app, which they can then use to share identity details with a wide network of different businesses who all accept that Digital ID Wallet.
2) Reusable digital identity account: this is a closed version of reusable digital identity where a business uses technology to verify the identity of their customer once, and then offers their customer a web-based way to re-authenticate their identity to that business. This could be with biometrics or simply a username and password.

Digital ID Wallets are very useful for the end user because they only need to verify themselves once and then use the same Digital ID again and again. So people can use their one Digital ID across a variety of use cases. This include buying age-restricted goods, accessing online services or proving their right to work.

For organisations, there is also a reduced risk of fraud as the user is verified to the highest level when they first create their Digital ID Wallet. With the quality and availability of fake IDs increasing, companies need to strengthen their identity checks and move away from simply checking an identity document.

Single entity reusable digital identities are used by businesses who want to be able to re-verify their customers without having to ask them to send over identity documents each time. A good example of this is in the background screening industry where a candidate may need to prove their identity.

For reusable Digital IDs to be truly valuable to the user, they need to be accepted as proof of identity and age in a significant number of places. For this to happen, it often requires new or updated regulation (as seen in the UK with the Digital Identity and Attributes Trust Framework). However, for significant adoption and retention, a regular utility is required, like using a Digital ID Wallet to prove age, qualifications and other credentials, or to access popular online services.

Core principles for a good digital ID

A ‘good’ digital ID will be built with the principles of privacy, security, and user control at its core, ensuring trust and accessibility for all users.

Privacy by design

- People should be able to use their digital ID to only need to show the required information, instead of showing a whole identity document. For instance, someone could show a verified ‘over 18’ proof of age to purchase an age-restricted item, without showing any other details.
- This gives them greater privacy and protection over their personal information.

Security

- Personal data should be protected with the strongest security.
- A secure digital identity system allows people to prove their identity without showing paper documents. This makes both online and offline interactions safer for individuals and businesses, striking a balance between privacy, security and convenience.

User controlled

- People should have control over their personal information. There’s an opportunity here to give them greater transparency over who has access to their data and limit the amount of information they share.
- They should also consent to share their data and choose what information to add to their digital ID.

Accessible and inclusive

- Everyone should have the option to prove who they are in a secure and easy way.
- A good digital ID will be flexible and inclusive. For instance, digital IDs should be available on different mobile operating systems. They should also accept different identity documents, so that even people without a passport can create and use a secure digital ID.
- There should also be non-digital alternatives available, giving everyone the chance to prove their age or identity in a way that feel comfortable to them.

Optional

- Digital IDs should always be optional because not everyone wants or has the means to use one.

Working with:

POST OFFICE
EasyID

YOTI
Yoti ID

LLOYDS BANK
SMART ID

Memberships, associations and accreditations:

WORLD ECONOMIC FORUM

FSM

WeProtect GLOBAL ALLIANCE

OSTIA ONLINE SAFETY TECH INDUSTRY ASSOCIATION

ISO 27001:2013 • ISO 27701:2019 CERTIFICATION intertek

ISO 27001:2013 CERTIFICATION intertek

ISO 9001:2015 CERTIFICATION intertek

SafetyTech Innovation Network

AICPA SOC 2

POINT DE CONTACT .NET

Reviewed by:

cdt CENTER FOR DEMOCRACY & TECHNOLOGY

Keele UNIVERSITY

Cigital

NIST

To find out more visit **yoti.com**