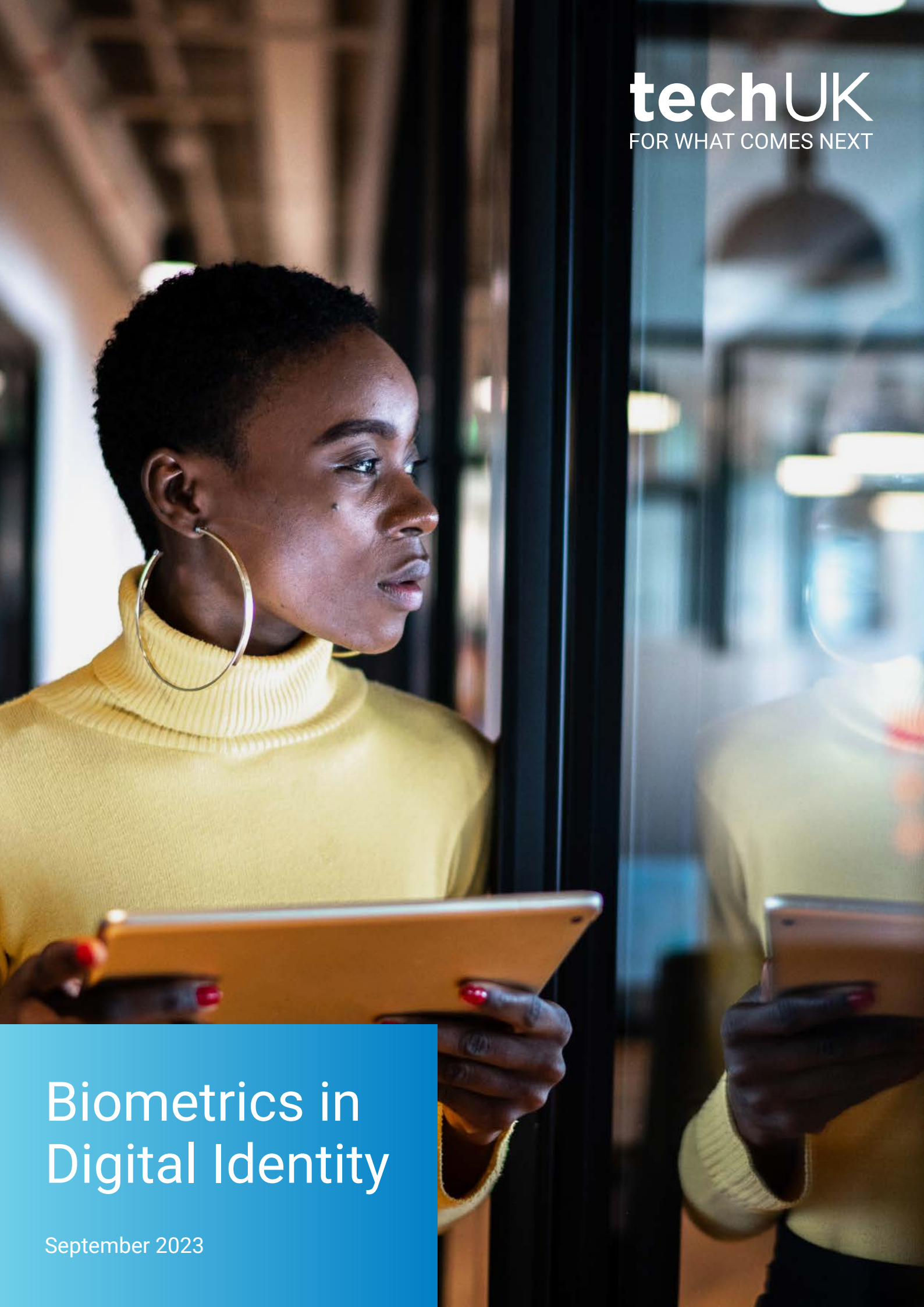
techUK
FOR WHAT COMES NEXT



Biometrics in Digital Identity

September 2023

Contents


Username
Password
Remember me
Forgot your password?
Login

Executive summary

The immediately obvious differential for any consumer using digital identity, and biometric data instead of existing, knowledge-based, manually-input, user name/password and additional multi-factor authentication safeguards (e.g. SMS) to either:

1. **onboard to an online service as a new customer**
2. **login to an online service as a returning customer**

is that the user experience is fast, convenient and secure, requiring little or no manual interaction.

The higher level of assurance inherent within properly implemented biometrics services can also play a significant part in developing trust in digital services by protecting both consumers and businesses reducing fraud and financial crime.

For businesses, biometrics allows them to streamline and simplify their internal operational processes, lower costs and concentrate resources on growing revenue.

Being able to quickly, conveniently and securely access government, banking and other online services, significantly reduce queues and traffic congestion in the travel and transport sectors and work from your home or other remote locations without the constant need to remember and manually input a myriad of different user names and passwords, these in turn being augmented by an additional security layer of multi-factor authentication in the form of SMS or email-generated security codes, authentication apps or similar is the nut that the digital industry has been trying to crack for a number of years now.

Remembering unique login details which might be used only once a year can prove problematic for citizens wanting to submit their annual tax return, the physical checking of paper documentation at airport check-ins and 'binding' of a ticket to an individual takes time, is susceptible to human error and can lead to the type of airport terminal congestion and

at passport control that we have all experienced. The disruption caused at Dover and other ports in recent years are another stark reminder of our continuing reliance on outmoded processes that depend on the production of correctly presented paper-based documentation and the negative impact it can inflict on the UK economy.

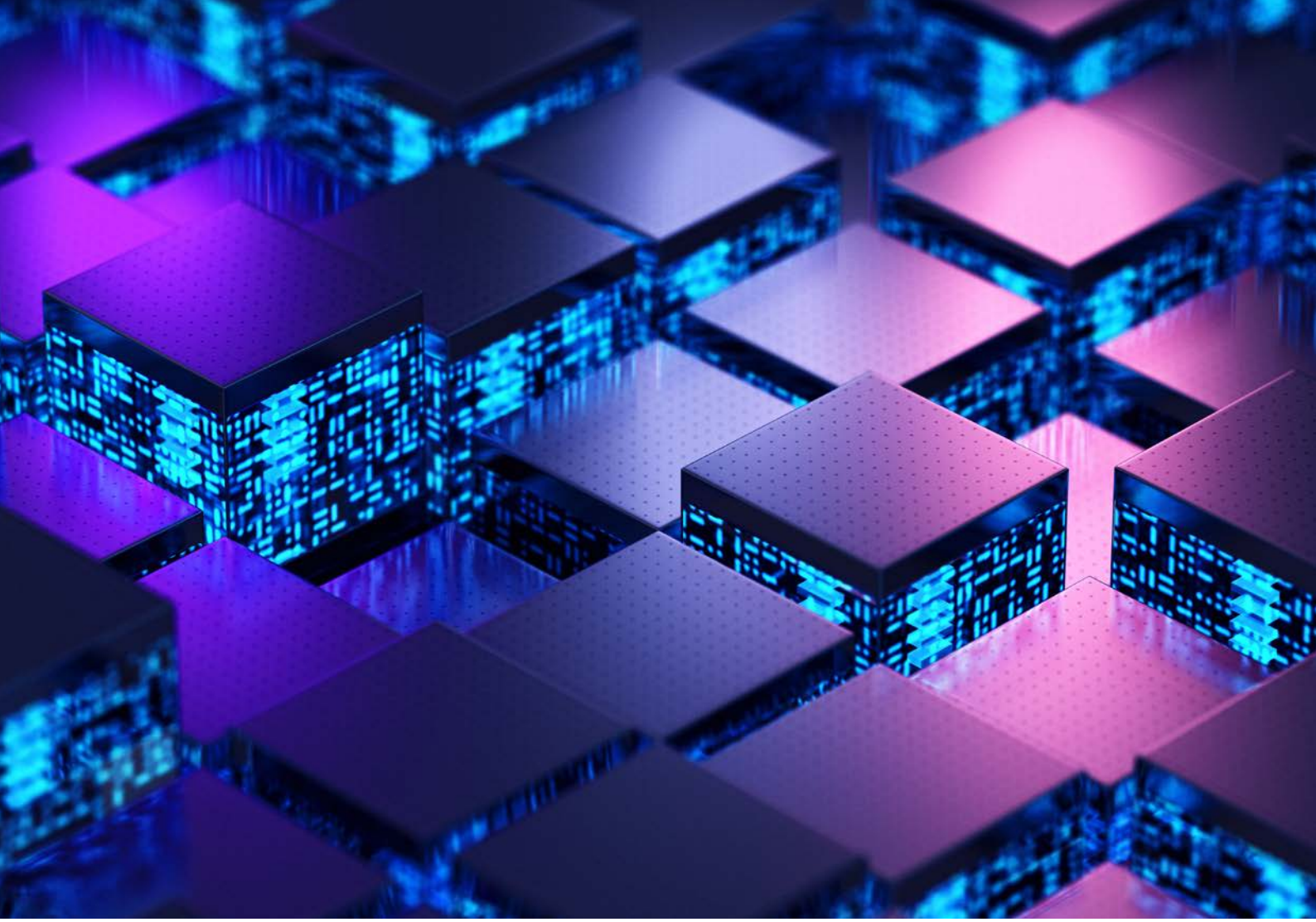
It is against this background that the advantages of implementing secure, high level of assurance biometric service platforms across both government and industry start to become clear.

Put simply, the use of biometric data, properly implemented can transform your customers onboarding and login experiences by removing almost all manual inputting of knowledge-based attributes such as user-names, passwords and security codes and doing so in a way that is significantly more secure – inherent in properly implemented biometric service platforms it is, by an order of magnitude, significantly more difficult for even the most organised and creative fraudsters to replicate (more on this in the report) - than any of these existing methods.

What the reader may not yet realise is the extent to which biometric data to verify and authenticate online has proliferated in recent years, particularly during the recent global epidemic which focused the minds of businesses and governments globally to accelerate the pace at which biometrics and other innovative technology could be adopted, with McKinsey reporting an overall seven-year increase in digital adoption as a direct result, even ten years in parts of Asia.[1]

Digital identity utilising biometric technology is today enabling individuals to identify themselves online or authenticate a transaction in much the same manner that we might previously have used a combination of username, password, memorable information, and multi-factor authentication. It is clear therefore that the increasing proliferation of biometric data as an attribute to verify and authenticate means the days of manually inputting usernames, passwords and additional, knowledge-based multi-factor authentication may soon be over entirely.

This innovative and transformative technology is freely available to many consumers today, most obviously in the online banking, health and travel sectors as demonstrated in the following chapter on Sector Case Studies. Perhaps the best-known example of this was the NHS's decision to incorporate biometrics (fingerprint and/or facial recognition) as a means of onboarding and accessing the NHS App.[2]



For individuals and businesses, the use of biometric attributes can deliver a significant uplift in the end-user experience without compromising on security and providing the higher level of assurance necessary to ensure that the person they are dealing with is indeed who they say they are.

Whilst the case for biometric identity verification and authentication has been extensively made already, more is required to accelerate adoption as the Government and businesses explore potential use cases and how to transition from legacy technologies. Given the clear benefits that digital identity solutions utilising biometric attributes can deliver to support individuals in their everyday lives, reduce fraud and increase the security of online transactions, it is vital that we find ways to accelerate adoption of this transformative technology.

The real-life case studies highlighted in this report are solving significant issues for end-users and business globally and clearly make the case for increased adoption of biometrics in more use cases across all sector verticals.

Introduction

Being able to prove that you are who you say you are or that you are entitled to access services in the real world can sometimes be challenging.

It may not be if you are merely collecting a parcel from your local post office perhaps, but if you are applying for a bank loan or trying to register for state benefits there will be a requirement to provide 'higher assurance' forms of documentation such as your passport, driving licence, a recent bank statement, council tax bill or similar.

For some in society, even this can be troublesome. Especially for the 17%[3] of UK citizens who don't possess a passport or the 26%[4] who don't have a driving licence. Add to this the inherent vulnerability of paper-based documentation such as bank statements, council tax or utility bills and the ability of criminals to fraudulently reproduce – forge - them to a much high standard over recent years and you have an increasingly difficult situation, for UK government, businesses and citizens alike.

Moving to a remote environment where proving who you are or what services you are entitled to access – and having others prove their identity to you in return –potentially expose individuals and businesses to identity theft and/or financial fraud by increasingly able criminal enterprises around the world.

This is the problem that the deployment of biometrics data and attributes, as an integral part of Digital ID solutions that deliver passwordless authentication, aspires to solve. The use of biometric data to confirm the identity of a remote user attempting to set up a new account, complete a transaction or even unlock their phone or laptop has proliferated in the past few years. Biometric data– be it the face and its inherent characteristics (physiognomy), the fingerprint, iris or retina, the voice, or even individual patterns of veins and arteries – act as identity attributes underpinning digital identity.

Right now, biometric attributes alongside digital identity technology are enabling a transformation in our remote engagement and creating a future where passwordless authentication is not just a possibility but a reality. As an example, since its launch in 2017 Apple has deployed its Face ID biometric solution to verify in-store transactions utilising the Apple Pay payment solution. Mastercard and many other financial institutions and banks globally have also launched, or are in the process of launching, their own biometric solutions to help fight the global increase in online fraud. Passwordless authentication is seen as an excellent mechanic to not only improve the customer experience, but also to increase authentication security and as a result help to reduce fraud.

Human nature being what it is, end-users often simply reuse the same, often amazingly simplistic, username & password combinations over and over across many different accounts and services resulting in inevitable security vulnerabilities. Recent research[5] into cybersecurity breaches revealed that nearly five million of these incidents happened due to the account password being (you guessed it) 'password'!

Within the UK public sector, biometric attributes are already being used in the delivery of secure public services to citizens. For example, the COVID-19 epidemic and subsequent increase in new users of the UK NHS App offered users (circa 30m registered to date) the ability to register using their NHS Login and a biometric process using 'liveness' technology. Also, in the transport and travel sectors, the application of biometric attributes is delivering significant improvements to passenger management at airports, train stations, and ports as well as the enhancement of the overall customer experience by reducing the need for a physical ticket, and passport and security checks.

At a time when we are seeing an increase in the number of powerful use cases of where this technology is making a difference to people in their everyday lives, the economic value of the market for biometrics technologies is also set to increase. According to a 2022 study by Transparency Market Research Inc. the global market for biometrics is growing fast and is projected to increase at a compound annual growth rate of circa 13% between 2022 and 2031 leading to a global market valuation of $136 billion.[6] In addition, a March 2023 report stated that the global market for Face and Voice Biometrics alone was worth an estimated $17.5 billion in 2022 and could reach $63 billion by 2030. Countries such as US and China are expected to be key markets for biometrics technologies. In Europe the EU Commission's push for the adoption of digital identity wallets, underpinned by eIDAS 2.0 regulation and across all 27 member states and large-scale pilots undertaken by consortia including techUK members is encouraging, though outmoded and insecure processes remain stubbornly prevalent in some major EU economies, such as using video calls to verify applicants for new bank accounts which are plainly sub-optimal and unlikely to meet the strict conditions set out in eIDAS 2.0.[7]

This economic optimism about the global potential of biometrics technologies to increase in economic potential seems to be reflected in the venture capital community with VC firms in 2022 reportedly keen to invest in biometrics start-ups and existing innovators in this space over the next two years.[8]

Given the economic potential and opportunities that the wider use of biometric technologies and solutions could unlock in the digital and wider economy, techUK believe it's vital that we consider now what needs to happen to encourage greater use of biometric attributes, how the UK can support the development of biometric-enabled passwordless authentication, and how current challenges or barriers that may be holding back the use of biometrics attributes, particularly in digital ID, can be overcome.

While this report does not examine the use of non-consensual use of biometrics technologies (such as Live Facial Recognition) by police forces and security agencies, it explores how and where the current adoption and use of consensual biometrics attributes and data is positioned already, and the future economic and social potential of these technologies should wider adoption accelerate.

Authors NB – it is important to note here the clear differential between the consensual and non-consensual use of biometrics.

This report is solely focused on use cases where the user consents to share certain biometric data as an attribute to verify or authenticate the identity of a remote individual in much the same way that the username and password methodology has been used historically and does not examine the use of biometric data in a non-consensual context, e.g., mass surveillance by police or security forces etc.

This report aims to drive debate and discussion on how the consensual use of biometric attributes and biometric-enabled technologies and solutions can be fully realised in the UK by:

- Explaining clearly what biometrics attributes are and how they work alongside digital identity solutions
- Making the case for why we need to increase the use of biometrics attributes for authentication
- Demonstrating real-life examples of biometrics data-driven technologies in action today in a number of key sectors including travel, transport, public sector, and financial services
- Identifying and exploring the challenges to greater use of biometrics data and technologies in the UK
- Busting many of the current myths around biometrics attributes that are driving the current narrative in the UK
- Recommending where action needs to be taken to overcome these challenges and increase the adoption and use of biometric attributes in the UK.

Definitions

What is biometric data, what are biometric attributes, what is passwordless authentication and what does this report cover?

Given the issues we are exploring in this report having clarity on the definition of the terms we are using is key. It is important to understand the following:

- What constitutes a digitally verified data attribute in the context of authentication?
- What is Verifiable Credential in the context of a Digital Wallet?
- What constitutes biometric attributes in the context of authentication that we are exploring in this report – namely the utilisation of biometric data for online authentication?
- How do biometric attributes and digital ID solutions work together?
- What is passwordless authentication and how is this enabled by biometrics attributes?
- The difference between fully consensual and non-consensual use of biometric data for authentication.

The following are the definitions and parameters that will be used throughout this report.

What constitutes a digitally verified data attribute in the context of authentication?

Simply put an individual's digital identity consists of digitally verified data attributes. This can range from something as simple as your name, address and date of birth. These might be best described as 'inherent' attributes. Other attributes such as your national insurance number is an 'assigned' attribute given to an individual.

What is a Verifiable Credential in the context of a Digital Wallet?

Put simply, a **verifiable credential** in this context is probably best described using the W3C definition in their 'Verifiable Credentials Data Model document[9] – 'A verifiable credential can represent all of the same information that a **physical credential** represents. The addition of technologies, such as digital signatures, makes **verifiable credentials** more tamper-evident and more trustworthy than their physical counterparts'

What is a biometric attribute?

Biometric data – be it the face and its inherent characteristics (physiognomy), the fingerprint, iris or retina, the voice or even individual patterns of veins and arteries – can act as identity attributes (a means of proving one's identity). This means your fingerprint or voice can be a biometric attribute that uniquely identifies an individual.

How do biometric attributes and Digital ID solutions work together?

Biometric attributes (such as facial data) can be shared by the end-user with their expressed consent for a specific, defined purpose to a Digital Identity Service Provider to enable the authentication of their identity via a digital identity solution, such as an app.

What is passwordless authentication and how is this enabled by biometrics attributes?

Passwordless authentication is where biometric data is shared by the end-user with their express consent for a specific, defined purpose to an Identity Service Provider to enable the authentication of their

identity. This replaces the need for a username and password. Your biometric data effectively becomes your password.

This can support online authentication and/or identification via a digital mechanism: e.g., opening a new online account (digital onboarding), returning to and accessing an existing online account or authorising an online transaction.

The most commonly used example of biometrics for passwordless-authentication are those utilising facial characteristics. However, biometrics data that can be used for authentication can also be an iris or retinae, voice, vein recognition as well as the historically familiar fingerprint. These are all individual and unique physical attributes that can be collected as digital data.

In facial biometrics, what is created is a proprietary, mathematical interpretation of the subject's face, called the facial "template". This facial template is proprietary to the facial recognition solution provider and is usually encoded with a security algorithm proprietary to that solution provider that is required to decode it. The vast majority of modern facial biometrics solutions use 'liveness' detection algorithms, designed to confirm that what is being seen or scanned is a real, live person and not a mask, copy or 'deepfake'. It is important to understand that it is the biometric data, and not the image itself, that is used in a passwordless-authentication context.

Difference between fully consensual and non-consensual use of biometric data for authentication.

This report is concerned solely with the fully consensual use of biometric data in a passwordless-authentication context to help identify an individual online or authenticate a transaction.

Where today we might use a combination of username, password, memorable information and multi-factor authentication to verify an individual's identity, an example of fully consensual use of biometric data is where an individual would consent to using their facial biometric data or fingerprint to unlock their phone, laptop or confirm an online mobile transaction.

As stated previously, this report does not examine the use of non-consensual use of biometrics by police and security or the use of non-consensual biometric enabled technologies such as Live Facial Recognition.

Why do we need biometric attributes for identification? The benefits of biometric attributes as an enabler of passwordless verification and authentication today

Being able to compare a person's face who is standing right in front of you with a document containing a photograph of that person and making a reasoned judgement as to whether or not they are who they purport to be has – along with handwriting/signature comparisons – been the de facto basis for personal identity assertion in the physical and remote worlds to date, albeit one that is inherently vulnerable[10] to document forgery as well as unavoidable, 'human error'.

The proliferation of devices, apps and online services that incorporate the use of biometric data to authenticate a person's identity over the past few years has therefore been a welcome development and regulatory reform in many jurisdictions will seek to hold platform providers more accountable than previously and to take proportionate, demonstrable action to protect their consumers from harm, particularly identity fraud with some platforms already taking action like LinkedIn's identity verification solution for US citizens.[11]

In the online world biometrics data has emerged as the solution to the long-standing username and password model for online authentication which has become an inefficient, insecure and outmoded approach to online identification and more importantly online security given the current cyber security threat environment. While two factor authentication and multi-factor authentication can provide added security, there are instances where the use of 2FA and MFA has led to customers and users experiencing 'drag' and a sub-optimal user experience when attempting to verify or authenticate remotely though many use cases exist where additional steps are deemed desirable, particularly for larger financial transactions, to instil in the end-user a sense of the importance associated with the transaction which some in the digital industry have started referring to as 'ceremony' but this is a matter for UX experts in their respective businesses and is not, nor should be associated with the technology itself.

The integrity, adaptability and accuracy of the best biometric applications available today allow for a user and customer experience that delivers significant advantages – for both the end-user and businesses – over other methods of remote onboarding or signing on to an existing online account, particularly those which still rely on some form of physical keyboard input from the user.

There are three key benefits to the use of biometrics in passwordless authentication;

1. **Security** – The US's National Institute of Standards & Technology tests on the top 150 biometric algorithms submitted achieved accuracy rates of 99%, with the top 20 achieving between 99.7% and 99.8%. and have so far have proved adaptable in the face of the evolving threat landscape, though deepfakes and synthetic identities are seen as the next threat against which solution providers must be vigilant.
2. **Customer or User Experience (CX/UX)** – For the end user used to manually entering their username and password, some memorable information and a multi-factor authenticator (SMS or similar), being able to achieve the same outcome with a one-step biometric solution delivers a far simpler and easier experience.
3. **Business Efficiencies** – Depending on the use case, efficiencies can be realised in different ways. For example, in 2020 FIDO Alliance research discovered that 58% of participants had abandoned online purchases because of forgotten passwords or unwillingness to open a new account requiring another username and password.[12] Other examples cite significant 'back office' efficiencies by removing the requirement for document processing and validation.


Now Boarding
Now Boarding
Group 1,2,3
EXIT
EXIT
RESTRICTED AREA
DO NOT ENTER

Biometrics in action | Sector case studies

The UK is fortunate to have many of the world's leading players in both the biometric and wider digital identity space who have proven very successful at exporting their solutions to other highly competitive markets abroad.

The following chapter demonstrates through real-life case studies how biometric attributes to enable passwordless authentication are already in use today and the value they can bring to customers and companies alike. We will be focus on the impact this technology is having in the following sectors and industries:

- Travel & Transport
- Public Sector
- Finance

As with other emerging technologies such as AI and digital ID, understanding the context in which technologies are being adopted and applied is vital. It helps to demonstrate the real-life benefits and value of using biometrics and the positive impact on real-world problems such as online fraud and the security of customers' data that biometrics attributes in action can enable.

Before exploring specific case studies of biometrics in action in these three sectors, we have provided an overview of the use of biometrics alongside technologies such as digital ID, in each of these sectors right now as well as relevant current developments that may impact greater adoption of these technologies and a snapshot of the value that the application of biometric attributes is bringing to people and organisations.

Travel and Transport

In April 2022 techUK held a webinar to explore the use of **Digital Identity in the Travel & Tourism Sector**. The focus of that session was the potentially transformative impact that effective use of biometrics data can bring to the overall travel experience of individuals and the opportunity to support an industry that is already undergoing a digital transformation. Speakers from **Condatis**, **iProov** and **Pegasus Aviation Advisors** brought to life how digital ID and biometrics data working together will be at the heart of the future of the transport and travel industry not only in the UK but globally and why it is important now that the UK finds way to encourage more use of this technology.

This message seems to be echoed by industry itself. In their **Global Passenger Survey for 2022** International Air Transport Association (IATA) found that the post-pandemic passenger's top priority is improved convenience when travelling. For example, the survey identified a willingness of passengers to share personal data via biometric technology platforms to expedite their airport experience. The survey also found that 1 in 3 had already used biometrics whilst travelling, 83% were willing to share passport, visa and health data and 75% were willing to use biometrics instead of physically producing passports and boarding passes. However, the same report also highlighted passenger concerns about how the safety of their data (56% concerned about their data being stolen via data breach), as well as how data was being processed, shared and managed (52% concerned about their limited knowledge of exactly who their data is being shared with and 51% do not understand how passenger data is handled/stored).

The IATA's survey results may well provide an insight into modern public perceptions of the potential of biometrics to significantly improve the individuals experience when travelling. However, it also highlights the need to address individuals concerns in relation to the security and privacy of their biometrics data when it is processed, stored and managed.

It would seem that the future of the use of biometrics in the travel sector is only likely to increase. The upcoming launch of the European Union's **EES Entry/ Exit System** (delayed until after the Paris Olympics in 2024) has been designed to modernise and improve the border management of EU Member States by significantly increasing the efficiency, quality and security of its border processes, whilst concurrently improving the travel experience for non-EU travellers. The question of how the introduction of how this EU system might impact UK and other non -EU travellers is at present unclear. However, what we do know is that the EU's EES system will, at the point of entry, collect and store personal data (including biometric) with this data processed, stored and managed under the EU's **Regulation 2017/2226.** Also, under the scheme if a traveller refuses to provide their personal data at the point of entry into an EU Member State, they will be denied entry and records of entries, exits and refusals of entry along with personal data will be kept by EES for a period of three to possibly five years.

This launch of this EU initiative provides a valuable insight into the importance that the EU attaches to significantly upgrading, modernising and optimising their border management systems. That the EU recognises the use of biometric data as a tool for achieving a significantly enhanced border management system provides an indication of how the future for this technology may develop across other jurisdictions globally.

The following are just some of the real-life use cases from the travel and transport sector that help to demonstrate exactly how the use of biometrics is already helping to transform both the travel experience of the end-user but also how business processes can be optimised and simplified delivering significant business process efficiencies.

Biometric Face Verification for Contactless & Ticketless Rail Travel

Overview

Eurostar wished to greatly enhance the customer experience for travellers between England and France on the international rail network. The challenge was to improve the throughput of large numbers of travellers through a number of security, immigration and ticket checkpoints. Aiming to optimise overall journey times, improve customer experience, whilst enabling an effortless “couch to carriage” travel process.

Following an Innovate UK-supported trial, iProov partnered with Entrust. iProov provide the biometric capability, Entrust built the app and ability to verify a passport and link the traveller’s ticket. This enabled a new face biometric travel corridor to be created, called SmartCheck.

Highlights

- Remote enrolment and verification of traveller - binding the traveller to their passport and ticket
- Enabling a contactless, ticketless, secure travel experience
- Operationally efficient, removing congestion from the concourse
- Optimising and enhancing the overall customer journey
- Safeguarding traveller privacy, meeting GDPR compliance

SmartCheck

Customer journey utilizing face biometric verification:

- Face Verification at Exit Check Control
- Passport Control
- Departure Lounge
- Face Verification at Ticket Gate
- Security and X-Ray
- Customer Enrol via App

Feedback

- 86% of respondents likely/very likely to use again
- 74% rated using the app as easy/very easy
- 67% rated the trial as good/very good

> ***“Face biometric technology is a fast and contactless solution which will enable secure passenger checks to take place more efficiently and provide a seamless start to the Eurostar customer journey.”***
> ***Gareth Williams - Strategy Director and Company Secretary, Eurostar***

WiBLE, a sustainable shared mobility company promotes more responsible mobility services to minimise the environmental impact. The company was launched in 2018 in Madrid with the aim to offer a sustainable zero-emission mobility alternative in urban settings. With a fleet comprising 500 KIA Niro plug-in hybrids the company enables its over 270,000 users to book, open and drive any available car. WiBLE is the first carsharing service to facilitate parking in the centre of Madrid, to save users' time.

The Challenge

As the first few years of WiBLE's existence coincided with the pandemic, the company focused on adapting to new business realities and evolving customer requirements. As a result, it introduced a new business model which brought cars to customers' doors – a strategy that allowed Wible to recover quickly and return to business earlier than expected. In line with the new strategy, the company wanted to streamline its user onboarding processes to facilitate an easy and seamless shared mobility service. WiBLE was in search of a partner who could accurately and reliably verify and authenticate users and their ID documents in a frictionless manner.

The Solution

WiBLE incorporated Facephi's biometric-based digital onboarding and authentication solutions to ensure new users are verified fast with a high level of accuracy. The solutions enable automatic document capture, remote user onboarding and authentication through selfies with passive liveness checks. To sign up for the WiBLE service, a user needs to download the app available with iOS or Android. Then the user needs to register an ID document and a driving license followed by a selfie. Facephi's digital onboarding solution automatically captures all the information on the documents with real-time OCR. Passive Liveness determines whether the user is a live person, countering risks of synthetic fraud or spoofing attempts. A matching algorithm then compares the selfie to the photo on the ID document, validating that the user is the person who he/she claims to be. The verification process takes only a matter of seconds.

Once the sign-up information is provided, the account is verified and activated automatically through the app within minutes. The user will receive a confirmation email once the WiBLE account has been activated. From that time on, the user can access the WiBLE app and start using the service.

The Results

With more than 2 million trips already, WiBLE is on a constant search to deliver the best possible solutions for users who want more flexible and greener mobility services.

Since the implementation of Facephi's biometric-based identity verification solutions, WiBLE has achieved a 40% reduction in user onboarding time. The company has also experienced a 50% drop in customer incident reports. WiBLE's main reason for choosing Facephi was the company's good experience with proof of life testing with Passive Liveness.

WiBLE aims to go beyond just delivering a shared mobility service, encouraging its users to join the challenge of a new urban mobility. A single vehicle can cover the mobility needs of many people, contributing to the sustainability of cities and reducing their environmental pollution. WiBLE's carsharing services offers them another possibility to use the car more efficiently.

Public Sector

Currently globally the use of biometrics in the delivery of public sector services is increasing. For example in India, users of the Aadhaar digital identity scheme can use their **biometric data as an authenticator**. In the US the Internal Revenue Service awarded an $86m contract for biometric identity verification services to allow taxpayers to set up and access their tax accounts and unemployment benefits using their biometric profile, and Singapore recently introduced the Multi-Modal Biometrics System (MMBS) to enhance security at airports, the system enables their border control function to capture iris, facial and/or fingerprints of arriving and departing traveller.

In the UK we have already seen the Home Office recognise the use of biometrics data and technologies in the EU Settlement Scheme. This example of biometrics in action by the Home Office is explored in more detail below. Within the NHS the COVID-19 epidemic and subsequent increase in new users of the UK NHS App offered users (circa 30m registered to date) the ability to register using their NHS Login and a biometric process using 'liveness' technology.

Right now, in the UK we are still seeing the ongoing development of a new single identity platform enabling citizens to interact with government digitally. The new One Login for Government will be *'a single, ubiquitous and simple way for people to log in and prove their identity when accessing online His Majesty's Government (HMG) services.'* One Login is being seen as a key deliverable in the Government Digital Services (GDS) work to deliver digital transformation across government departments. For example, HMRC recently announced that they would begin to migrate users to One Login away from Government Gateway from summer 2023.

The UK Government Digital Service's (GDS) One Login platform has recently awarded a £5m contract for a biometric front-end solution. In addition, providers to OneLogin including Experian, iProov and Hippo Digital, Deloitte have been awarded the contract to provide the OneLogin app which, according to the contract notice published in November 2022, will use near-field communication (NFC) technology for scanning of documents containing biometric chips, such as passports.

In addition to OneLogin, the UK government's UK Digital Identity and Trust Attribute Framework[13] (the UKDIATF, now in Beta since April 2022) will provide the regulatory basis for the development of the private sector digital identity ecosystem in the UK. The Framework has an important role to play in supporting and enabling the increased adoption and use of biometrics attributes to support digital ID solutions and therefore techUK is urging the government to finalise the Trust Framework by the end of 2023.

The following provide real-life use cases from the public sector bodies in the UK and beyond where biometrics data and data-driven solutions are demonstrating real impact and supporting public sector organisations to achieve their aims and objectives. These examples bring to life what biometrics data in action can mean to the public sector.

Overview

Sopra Steria's innovative approach to linking biometric technology with prison appointment systems has transformed how Northern Ireland Prison Services (NIPS) manages the movement of prisoners in its high security environments. Prisoners are empowered to move securely within prison buildings independently, which has freed up vital time for staff to focus on rehabilitation and preventing reoffending.

The Northern Ireland Prison Service works across three differing operational environments: High-security, medium-security and specialist Young Offenders' Provision. The ultimate aim of the service is to improve public safety by reducing the risk of reoffending through the management and rehabilitation of offenders in custody.

Challenge

To protect the safety and security of the public, prison colleagues and inmates, it is paramount that NIPS can verify the identity of every individual moving through its prison sites.

Specifically, NIPS required a more efficient way to move inmates through its sites and access accurate real-time data about the exact location of individuals, where they have been and when.

At peak times, prison staff need to manage and oversee the movement of large groups of prisoners, sometimes up to 300 people. This could be when prisoners are moving from one area to another to take part in activities, medical appointments or leisure time. The prison population in Northern Ireland is diverse, for instance a significant proportion do not speak English as their first language.

When it came to managing appointments, the organisation needed to modernise an admin-heavy system which required printing out appointment details, manually updating a database and physically escorting prisoners from a residential area to another location such as an activity centre. For the highest security, they needed live, real-time data about where all individuals were at any one time and this wasn't possible with the historic paper-based and manual data-entry systems.

Solution

Sopra Steria partnered with fellow criminal justice innovators, Lava Group, to develop a bespoke identification and verification system for NIPS. Today, any individual entering one of the prison establishments will have their identity documents scanned and verified once andwill have their photograph and biometric fingerprints taken. The information is instantly stored on a secure database and updates the central Causeway system used across criminal justice organisations in Northern Ireland.

Uniquely, the intuitive system is linked directly to the prisons' appointments system. Inmates' movements can be controlled and managed through this innovative combination of biometrics technologies and digital calendars. This means that prisoners no longer need to be escorted by prison officers from residential areas to appointments and activities. Inmates simply use their contactless ID cards and scan their fingerprint. If it is time for their appointment and they are who they say they are, the system will let them through the secure turnstile.

Sopra Steria ensured that information and guidance was available in all required languages and also in graphic form to cater to every individual using the system. This system also provides management staff with live, real-time data about people's movements and exact locations. They can instantly see whether people are in transport and if they are in the correct area. It is a priority for NIPS to encourage prisoners to engage in activities which support their rehabilitation. This innovative use of technology makes it significantly easier for the prisons to facilitate this in a controlled way, which ultimately benefits prison populations and colleagues.

Not only does this empower the 95 per cent of inmates who are able to move freely around the prisons, but it also means officers can focus their attention on the rehabilitation priority rather thanmenial and administration tasks.

Results and Benefits

- Prison officers are no longer required to accompany every inmate to activities and appointments, reducing pressure on resources.
- Through detailed data analytics, the system can also be used to monitor and track other activity. For instance, the information available could be used for contact tracing to prevent the spread of diseases such as Covid-19.
- Real-time information and an accurate record of prisoner location, aids the management of prisoner activities and appointments.
- Greater control of an inmate's movement, where exit from and entry into specific areas is based on scheduled activities.

Feedback

> *"Sopra Steria has done an incredible job implementing a truly transformational digital project. Whilst the pilot is still at an early stage, it is working which is already an amazing result delivered by a partnership."*
>
> *Robbie Burrows, Head of NIPS ICT Services at Department of Justice*

EU Settlement Scheme

Overview

Following the UK's decision to leave the European Union, the Home Office set out to create a simple application process allowing 4.2 million EEA nationals to apply to the EU Settlement Scheme.

Applicants need to complete just three key steps – prove their identity, show that they live in the UK, and declare any criminal convictions. To make this as simple as possible, the Home Office sought out new innovative capabilities to create an optional end-to-end digital application channel.

iProov worked with Entrust Software and Inverid to deliver a scalable, secure and usable solution. The details of the project can be seen in this case study from Entrust.

The app enables EEA nationals living in the UK to complete an application in under 10 minutes, using the following innovations to ensure high levels of identity assurance:

- Remote identity documentation checking using the Inverid solution. Passports, driver's licenses, or other ID credentials can be scanned using a phone using either near field communication (NFC) to read the chip in the document, or optical character recognition (OCR) which reads information from a photo of the document.
- Biometric identity authentication using iProov's Genuine Presence Assurance technology to ensure that the person is the right person, a real person, and authenticating right now.

Recent demands for innovative technology to help deliver a simple application process for EEA nationals to apply for EU Settlement Scheme status has proved very effective in streamlining both the application process itself and, crucially, the Home Office internal business processes that previously relied on the provision and checking of physical documentation saving valuable human and financial resources in the process.

Highlights

- More than 4.2 million applications have been successfully concluded.
- A high percentage completed their application in under 10 minutes, with a high level of identity assurance.
- Over 2,300 different makes and models of Android and iOS devices have been used to complete the identity verification process.
- Peaks of 25,000-30,000 applications per day have been supported.

Feedback

In a 2019 EUSS survey, 79% of applicants indicated that proving their identity through the app was either "very easy" or "fairly easy". A further 7% found it neither difficult nor easy.

Singapore Government – National Identity Programme

Overview

Four million Singapore residents can now access digital government services online using facial verification implemented by iProov and Toppan Ecquaria for the Government Technology Agency of Singapore (GovTech) under the pioneering National Digital Identity (NDI) program. GovTech is the government agency driving Singapore's digital government transformation and Smart Nation initiative.

iProov and Toppan Ecquaria, a digital transformation company, were selected following an open international tender and many months of user testing and intensive security evaluation.

The system automatically enables four million SingPass users to authenticate themselves and prove that they are genuinely present when accessing online government services on personal devices or at kiosks. Activities such as completing a tax return can now be completed with a simple facial biometric scan, replacing the need to remember passwords. SingPass is every Singapore resident's digital identity. It has evolved into a gateway allowing convenient and secure access to over 500 digital services offered by more than 180 government agencies and commercial entities.

Singapore is already allowing private sector organizations to leverage the government-built identity infrastructure for SingPass. Banks and other businesses, large and small, can securely integrate with SingPass Face Verification, to offer world-class online customer authentication capabilities without the cost of building their own systems. It marks the first time that cloud facial verification, provided by iProov, has been used to secure national digital identity.

For Singapore residents, the ability to register for a bank account or engage with other organizations using the SingPass Face Verification offers a number of benefits. As well as access to a wider range of digital services, the user sees greater convenience, a simplified user experience, and increased privacy and security, as they no longer need to set up passwords or share sensitive data with every individual company. Such improvements in accessibility and online trust will lead to greater uptake of digital services, one of the aims of Singapore's Smart Nation initiative.

Unlike face recognition, which matches a physical face seen in a crowd to a list of images on a database, face verification is done with the knowledge and collaboration of the user. iProov's Genuine Presence Assurance technology uses a facial biometric scan that is highly secure, yet effortless to use. The camera on the mobile device, computer or kiosk scans the user's face while the screen illuminates with a sequence of colours for a few seconds. This confirms that a user is the right person (the rightful holder of their national identity number); a real person (not a photograph, mask or digital spoof); and authenticating right now (not a deepfake or injected video).

The cutting-edge solution of iProov facial biometric authentication and Ecquaria Government Platform Suite will augment and replace a device-based security solution, which uses SMS one-time passcodes. The new approach provides a secure, cloud-native solution that benefits citizens, businesses and government agencies in Singapore.

Highlights

The face verification solution:

- Is simple to use - a brief face biometric scan requires no effort from the user. As it compares the user's physical face to the image held in the Government biometric database, the user does not have to enrol in the program.
- Increases accessibility by encouraging Singaporeans, especially older residents with limited mobility, to use online banking and other services.
- Improves inclusivity to those without smartphones, by extending the service to Government agencies' kiosks.
- Gives private businesses, both large and small, the ability to grow their digital services without needing to build their own infrastructures and biometric database.
- Grows the digital economy by encouraging uptake and use of online services, both from government and private businesses.
- Increases security - passwords and other credentials stolen through phishing attacks will be useless as Genuine Presence Assurance checks that the individual is the right person, real person, authenticating right now.
- Reduces the need for password and reset administration.
- Improves convenience for millions of Singapore residents, who will be able to easily and securely access government and business services online using their existing national identity.

Feedback

> ***"Singapore's national digital identity, SingPass, enables citizens and permanent residents to transact seamlessly and securely with public and private sectors' digital services. We recently introduced a new biometrics face verification service for users to log in more conveniently to digital services, whilst providing an added layer of security for government agencies and businesses. SingPass Face Verification, under our National Digital Identity (NDI) program, will help partners enhance their customer service journeys. We will continue to extend useful and trusted NDI services to more private sector organizations to accelerate digitalization and grow Singapore's digital economy."***
>
> ***Quek Sin Kwok, Senior Director of National Digital Identity at GovTech Singapore***

Australian Government – Liveness Solution for Digital Identity

Overview

Millions of Australians will soon be able to access digital government services online after proving their identity using face verification from biometric authentication leaders, iProov. Following an open tender process, iProov was selected to provide a liveness solution for myGovID.

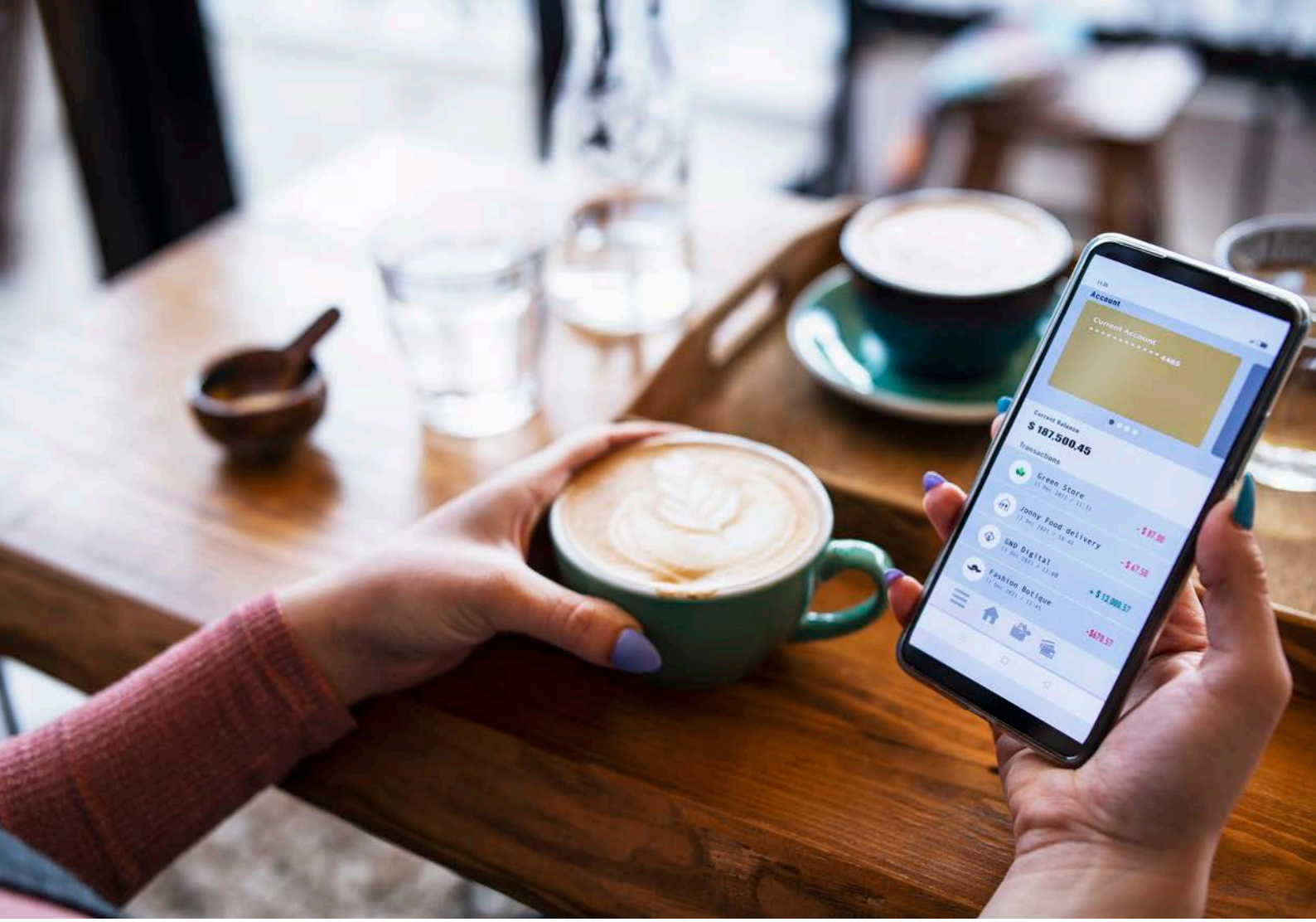
iProov's Genuine Presence Assurance technology will enable Australians to set up their myGovID digital identity using a simple face scan on their mobile devices. This will provide access to a range of services, including managing tax returns, accessing health services and applying for benefits.

Unlike face recognition, which matches a physical face seen in a crowd to a list of images on a database, face verification is done with the knowledge and collaboration of the user. iProov's Genuine Presence Assurance uses a facial biometric scan that is highly secure, yet effortless to use on any personal device.

Highlights

This Genuine Presence Assurance process delivers a multitude of benefits including:

- Simple and inclusive to use - a brief, passive face biometric scan requires no effort from the user. No need for movement, following instructions or other skills
- Inclusive to access - works on any device and is not dependent upon any particular brand or model
- Convenient - enables users to access more services securely online reducing the need for visits to shopfronts or phone calls.
- Secure – protects against identity theft by preventing impersonation or the use of copies of victims' faces
- Resilient – actively mitigates risks from emerging threats
- Privacy is maximized and respected - user data is fully protected
- Encourages growth of Australia's digital economy by increasing uptake and use of online services



Financial Services

The financial services industry has embraced the use of biometrics data, particularly the use of facial, fingerprint and voice data, perhaps more than any other, so far. For example, today many of us use a banking app either via our phone, a tablet or computer that in many cases we will have logged onto using either fingerprint or facial biometrics and have been doing so for some time now.

As with digital identity technology itself, UK banks are well placed to help drive the wider acceptance and adoption of biometrics technologies and the shift to passworldless authentication and have the resources to help achieve this. Therefore, if the UK is to encourage greater adoption and use of these technologies closer cooperation between the UK banks that are fighting fraud, which has risen sharply during the COVID-19 pandemic, would be a welcome development and could help to drive greater take-up and use by other sectors and industries that are also facing challenges related to fraud, the security of personal data and cyber security.

The recent announcement of the partnership between Lloyds Bank and digital ID provider YOTI to support the development of secure financial services is an example of where this is already happening in the **financial services market**.

The following examples of the use of biometrics data-driven technologies in the global financial services sector show how these technologies are already being used to increase the customers' experience and overcome challenges facing this industry.

Namutek – Biometric Identity Verification

Namutek is a Central American Fintech company that produced the region's first p2p mobile app, Kash. Founded in 2019, Kash enables p2p financial transfers, regardless of bank, time, location, or even whether the recipient has the application installed, and supports Visa and Mastercard.

This new product arrived at a time of rapid technological advances, heightened by the recent pandemic. In the post-pandemic world, the banking sector has had to strive even hard to remain competitive, by adapting to challenging new circumstances. In order to stand out, investing in cutting-edge technology is no longer just an option, but a requirement. Fraud, which has always been a concern, is today a major threat that manifests itself in a multitude of ways. Strengthening security measures to continue to protect customers and their assets is therefore of paramount importance.

Kash, naturally, has to deal with all the risks that come with being a transactional application. Security is one of the most important cornerstones of the brand, so it cannot afford to put its customers or their money at risk. The security system must be robust and combat fraud effectively so that users can use the platform without concern. To achieve this, digital identity verification through biometrics was key to strengthening the security of the application and customer data.

In the first two years, when they were making a name for themselves in the sector, they used their own technology. However, as the number of users grew, these solutions gradually ceased to be efficient, and a new system was urgently required. If they wanted to become a benchmark for instant transactions, they would need to turn to an expert in digital identity verification with significant experience in the banking and Fintech sector. The solution would also have to recognise documents in a variety of different formats and require minimal input from the user.

Although they considered several possibilities, Facephi fit the bill perfectly, with a long and successful track record, not only in the sector but also in the territory. Facephi's technology is designed to bridge geographical and generational differences and continues to be enhanced for a more comfortable and efficient experience. As users enjoy optimal user experiences, retention rates remain high.

Before Facephi, the Kash team handled customer security verification processes manually, which was costly in time and resources. However, following the application of Facephi's solution, manual customer verification was reduced by 30%. The end-user also benefitted from significantly faster, easier, and more secure transactions.

Banco del Pacifico – Biometric Identity Verification

Banco del Pacifico partnered with Facephi to facilitate secure biometric identity verification and authentication for streamlined customer onboarding, account logins, access to other banking services and more.

The Challenge

Banco del Pacifico's processes were originally encumbered by major manual inefficiencies to achieve KYC compliance. The bank's clientele was contacted by cold calls and often required to visit the branches in person to complete customer due diligence procedures. This placed a significant dampener on onboarding rates while increasing operating costs. The goal was to have a transparent and easy process so that anyone could have a savings account without complications. In order to optimise KYC procedures and facilitate remote onboarding and account management, Banco del Pacifico required a complete digital transformation of all processes.

The Solution

Banco del Pacifico incorporated Facephi's biometric-based digital onboarding solution to facilitate easy, fast, and compliant account creation. New members can join the bank remotely from anywhere by just scanning their ID documents and then taking a corroborative selfie.

Facephi's digital onboarding solution automatically captures all the information on the ID document with real-time OCR. Passive Liveness technology determines whether the user taking a selfie is a live person, countering any risk of synthetic fraud or spoofing attempts. A matching algorithm then compares the selfie to the photo on the ID document, validating that the user is who he/she claims to be. The verification process only takes a few seconds, and all user data is securely encrypted.

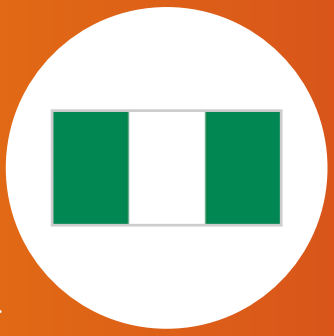
Once the sign-up information is provided, the bank reviews the data and checks its veracity with the Ecuadorian Civil Registry, to ensure the user is whom he/she claims to be.

The Results

For the initial trial, Banco del Pacifico started with a package for 50,000 account openings with the aim to onboard just 5% of its new customers with Facephi's digital onboarding technology. But in less than two years, Banco del Pacifico had expanded to 250,000 account openings and was onboarding 75% of its clientele remotely with the digital identity verification solution.

Testament to the new digital processes' user-friendliness was the fact that "only" 50% of new customers were "millennials". The other 50% were older generations that are usually less likely to use remote digital services but adopted the new processes due to their intuitive design and ease of use.

As a direct result of this digital transformation, Banco del Pacifico is today recognised as a regional banking pioneer with the best user experience. This was reflected by the Fintech Americas award they received in 2019. Moreover, by adopting Facephi's digital identity verification solution, Banco del Pacifico slashed operating costs by 60%, while maintaining easy KYC compliance.



Nigeria (Government Pensions) – Biometric Identity Verification

A large government organisation in Nigeria plans to introduce a pension collection app with an integrated digital identity verification service to enable pensioners to self-onboard, verify their identity and access their pension entitlement safely and quickly, while protecting the organisation and pensioners from potential cases of fraud and identity theft. As it is more challenging to prove identity digitally, this is where Afrilight and Facephi have taken on the task.

The Challenge

The organisation requires the following to be performed remotely:

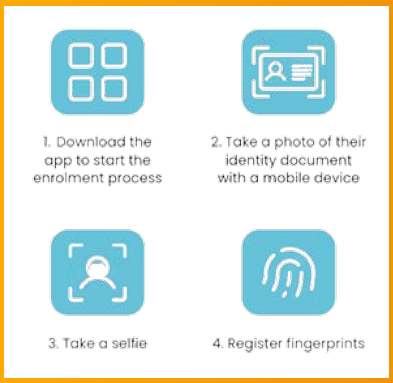
Verification of identity. As a part of the onboarding process, pensioners must take a photo of themselves, register a fingerprint, and provide an ID document (e.g., passport, a driving license) to validate their identity.

Proof of life. Pensioners must prove that their identity document belongs to a live person in presence. For this, they are required to visit a bank branch and present their ID documents in person where a bank employee evaluates the documents and confirms that the retired citizen is indeed the person who he/she claims to be and only after that access to the entitlement is granted. With the new process, this requirement will need to be performed remotely and securely.

Authentication and record keeping. Pensioners should verify their identity before accessing their pension entitlement through the app. Once confirmed, the app should transfer the results to the government authority database for keeping the pension scheme data up to date.

The Solution

Afrilight and Facephi have partnered to develop a reliable pensions collection app with integrated biometric-based digital identity verification technology. The app addresses the government organisation's challenges in the following way: senior citizens are enabled to remotely onboard themselves with a pension service. They are required to follow these steps:



Facephi's digital identity verification solution leverages advanced OCR to extract the document data in real-time, matches the selfie of the person to the photo on the ID document, as well as reliably registers fingerprints for future authentication requirements. Passive Liveness technique determines proof of life with minimal interaction from a senior citizen. All that is needed is a simple selfie taken with their mobile device from anywhere, reducing time and effort.

For further entitlement claims, pensioners are required to take a quick selfie and a fingerprint scan to verify their identity against their previously registered biometric credentials. Once complete, the app also triggers instant communication to the relevant servers to keep the person enrolled on the organisation's pension database. The enrolment process is quick, accurate and seamless.

In addition, the app considers several specific angles:

- **Technology.** The app can evaluate Wi-Fi connections and the types of devices pensioners use. For example, the app works reliably on all devices that are up to eight years old. It has been a significant element to consider during the development process, given that retired citizens use a variety of mobile devices and in most cases, they are not the recently made models.

- **User Experience.** The new app is designed for +60-year-old retired citizens, some of whom might not be as digitally advanced as others. Therefore, the user experience has been designed to be intuitive and seamless. In this perspective, the digital identity verification process requires minimal cooperation from an end user – just a simple selfie and a fingerprint scan. The technology takes care of the rest.

- **AI Bias.** With the widespread challenge of bias in AI, it is crucial that the app's facial verification systems eliminate any potential demographic bias problems. Due to Facephi's extensive work in the biometric facial verification space across Latin America, Asia and Africa, its diverse datasets provide a solid foundation for stringent training of the AI systems to deliver the most accurate results. These tests prove the robustness of Facephi's technology with a 99,998% hit rate. Afrilight and Facephi have developed an outstanding pension collection app addressing the requirements of the government organisation. The app offers a superior customer experience and a higher level of protection to prevent and combat potential cases of pension fraud and identity theft.

Challenges

Before looking at the challenges and barriers that may be preventing greater use of biometric attributes for authentication in the UK, it is important to consider the factors that are key to the successful deployment and adoption. From the examples of existing uses of solutions enabled by biometric technologies outlined in this report there appear to be at least three key factors that are important in enabling a successful deployment and use of biometric attributes-enabled digital identity solutions. These are:

1. **A strong need and market demand for a biometrics service or solution**

   For example, where the use of biometrics data is needed to address a specific problem or need. The exponential growth in registrants for the NHS App during the pandemic reflected users' desire for the NHS COVID Pass to illustrate their COVID-19 status during the pandemic as well as their interest in easily accessing their own medical records online.

2. **Both the technology and the organisation implementing the technology must be trusted by users**

   As the success of 30+ million registered users of the NHS App during the COVID-19 pandemic proved, a trusted brand or organisation utilising this technology in a way that put the needs of users at the heart of the solution can achieve spectacular results.

   However, the recent increase in the availability of generative AI to create fake imagery, even to create seemingly live and authentic-feeling conversations in real-time could constitute a significant problem for governments and business alike, as human-based systems simply won't be able to distinguish between what is real and what is not in this scenario. It is therefore critical for any system utilising biometric data as a front-end authentication mechanic utilise robust and tested 'liveness' and AI techniques and technology as a combative and adaptive response.

3. **The service must have the potential to scale**

   This means a service must be available to all in any domestic market. Of course, for any new technology to truly scale, then global operation and interoperability is important.

While these may be key success factors that can help the increased use of biometric data attributes there are challenges and barriers that are seen to be holding back greater adoption across industries and sectors. This chapter aims to identify and explain the core three challenges techUK believe is holding back the increased use of biometric technologies, and therefore the adoption of passwordless authentication solutions. We also offer recommendations on how these barriers could be overcome. The three key challenges are:

1. **Enabling a thriving UK digital ID ecosystem through a clear and robust regulatory framework**
2. **Current public narrative and messaging around biometric technologies**
3. **Public trust and confidence in biometrics**

Current public narrative and messaging around biometric technologies

As stated earlier, this report is concerned solely with the fully consensual use of biometric data in a passwordless-authentication context to help identify an individual online or authenticate a transaction. For example, in much the same manner that today we are using a combination of username, password, memorable information, and multi-factor authentication to achieve the same outcome. This report does not examine the use of non-consensual use of biometrics by police and security agencies for mass surveillance.

It is important to make that distinction, as there continues to be a lack of clarity around the difference between consensual and non-consensual use of biometrics in the current public debate and narrative around biometrics data and technologies. This lack of clarity leads to headlines and media reports confusing the way biometrics data is used and by whom. As a result, the public debate and discussion around biometrics becomes confused and the real-life positive use cases and examples of biometrics, alongside technology such as digital ID, is lost in the noise. As a result, this is likely to hold back demand by the public for this technology and therefore limit adoption and take up in the UK.

Facial biometrics has provided the editors of global media outlets with an easy target in recent years. They have attempted to provoke public sentiment and emotion with often poorly researched, biased reporting clearly aimed at generating an attention-grabbing headline rather than enabling a greater understanding of the technology.

The public narrative around biometric attributes that enable digital identity and a shift to passwordless authentication must be changed. To do that we must identify and address the misunderstanding that exists around the consensual use of biometrics data and what it means to people and organisations. We must bust the myths that exist right now if we are to change the public narratives to focus on the positive potential of biometrics and encourage greater take-up and adoption at scale in the UK.

It is worth noting here that many use cases do not always require the service owner to know the identity of any individual end-user, rather that they need to verify that the person presenting themselves in a remote interaction has specific permissions or access requirements.

The lack of distinction between the consensual, user-initiated presentation of biometric data in preference to the manual inputting of a username and password to onboard and access online accounts and services and non-consensual, mass media surveillance where individuals can be identified by the police and security agencies using their facial biometrics has not helped the public gain a better understanding of the benefits of biometrics as a digital identity attribute.

We must examine the issue of public trust in biometrics and what industry and government can do to help the public feel more secure in using this technology below however what is clear is the need to counter the - often misleading - media narrative around biometrics data, that often blurs the distinction between the user-initiated, consensual use of biometric attributes to verify and/or authenticate a person's identity with non-consensual, mass surveillance use of biometrics to identify an individual person or group of persons in a public space without their prior consent.

Public trust and confidence in biometrics

The issue of public trust and confidence in the use of personal data continues to be a factor in the acceptance and uptake of technologies including AI, cloud and digital ID. To ensure public trust and confidence in emerging technologies can be achieved

it's important to firstly understand and identify the concerns that may be holding back public trust.

For example, as mentioned earlier in this report, within the travel and transport sector the International Air Transport Association (IATA) found in their annual Global Passenger Survey for 2022 that respondents had significant concerns over the use of their personal data, the lack of transparency around who and why their data is shared, processed and stored and what the potential implications are for them as individuals.

However, a study[14] by Visa in the US published in October 2022 showed that roughly half of the consumers interviewed indicated that they would switch away from a card network, bank, or mobile phone provider that doesn't offer biometric authentication in the future. Therefore, there are signs that public trust in digital solutions that are enabled by biometrics attributes can be gained and achieved. techUK member Callsign's recent report 'The Digital Trust Index'[15] also found that there is a significant consumer appetite for digital identity to help protect them whilst interacting and transacting online. The report also made the case that positive, measurable gains in public trust in digital services will have a directly corresponding impact on GDP per capita according to their analysis. So, the question then becomes how to move forward and build public trust in biometrics.

Given the potential benefits to individuals in their everyday lives from the use of biometric attributes to enable authentication and help to protect individuals and their data, it is important that the right approaches and solutions are found to identify and address the issues that may be preventing greater public trust and confidence in biometric attributes and technologies.

Fundamentally, the use of biometric data in our daily lives will be determined by the public's trust in the efficacy of the governance structures around

biometrics and the security it provides around privacy. With this in mind, the good news is that UK GDPR clearly addresses biometrics data and the requirements that organisations must adhere to. For example, the UK GDPR defines biometric data in Article 4(14). It states that:

'Biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic (fingerprint) data.

In addition, biometric data is classified as 'Special Category Data' under UK GDPR alongside personal data sets revealing or concerning a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetics, health, sex life and/or sexual orientation.

techUK members believe that UK data protection legislation adequately addressed the specific requirements related to biometric data and that the law currently provides sufficient protection for end-users. Therefore, rather than the need for additional legislation in this area, we believe greater awareness, particularly amongst potential users of biometric data-driven technologies and solutions, is needed to address any specific data protection and privacy issues or concerns individuals may have.

The announcement that the UK ICO is planning to release specific guidance on the use of biometrics in 2023 is welcomed as a way to address any concerns in this area and build greater confidence in how biometrics can be used and applied. techUK and its Digital Programme Working Group look forward to engaging with the ICO on this guidance to help overcome any existing barriers and promote greater uptake of this technology.

Enabling a thriving UK digital ID ecosystem through a clear regulatory environment

Digital identity is the foundation stone for the use of biometric attributes for authentication. techUK believes that a thriving digital identity ecosystem is predicated upon a clear and robust regulatory environment.

The UK Government's UK Digital Identity and Trust Attribute Framework[16] (the UKDIATF, now in Beta since April 2022) will provide the regulatory basis for the development of the private sector digital identity ecosystem in the UK and is key to ensuring that digital ID ecosystem and market in the UK can thrive. techUK, therefore, calls on UK Government to;

- Deliver the UK Digital Identity & Attributes Trust Framework by the end of 2023
- Ensure that it is practical, proportionate and pro-innovation
- Put digital identity at the core of a clear industrial policy on science, innovation & technology and communicate that vision to the electorate, to industry, and to our trading partners globally
- Ensure regulatory coherence and coordination across government on biometrics and digital identity
- Work closer with other countries on international interoperability. and technical standards

techUK will also continue to work with its members, government, and other UK stakeholders from both the public and private sectors to help create the best digital identity ecosystem possible with technology that delivers concrete benefits for UK citizens and a regulatory environment that is effective, flexible, proportionate and the continues to encourage UK technological innovation.

Conclusions

It is clear that individuals and organisations can benefit from increased adoption of biometrics as an enabler of passwordless authentication both in terms of security and ease of use.

Right now, it is both exciting and encouraging that many of the best biometrics solution providers are partnering with other technology specialists to deliver robust, best-in-class digital identity solutions for the private and public sector alike. This is a clear indicator of an industry sector working together to deliver flexible, adaptable, and secure technology solutions to its customers in the spirit of healthy competition.

The real-life examples and case studies of biometrics in action outlined in this report clearly show what is possible today if this technology is embraced, harnessed, and scaled effectively. What is now needed is action to address the challenges that may be preventing the benefits of this technology from being felt more widely.

Given the economic potential of the global biometrics market further underpinning the digital identity industry, the UK cannot afford to be left behind. We must find ways to get the public narrative right so we can increase public trust in these technologies and help support the development of a thriving digital ID market across the whole of the UK.

techUK stands ready to help make this happen. Through our Digital ID programme, we will continue to act as a convenor bringing together policymakers and industry leaders in biometrics, digital ID, and other technologies such as PETs, to help shine a light on the economic and social potential of biometrics and how biometrics attributes can help move the UK forward into its digital future in a way that is supported and secured by passwordless authentication.

References

1. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Strategy%20and%20Corporate%20Finance/Our%20Insights/How%20COVID%2019%20has%20pushed%20companies%20over%20the%20technology%20tipping%20point%20and%20transformed%20business%20forever/How-COVID-19-has-pushed-companies-over-the%20technology%20tipping-point-final.pdf
2. https://digital.nhs.uk/services/nhs-app/nhs-app-strategy/making-features-of-the-nhs-app-available-for-wider-use
3. https://www.ons.gov.uk/peoplepopulationandcommunity/populationandmigration/populationestimates/articles/detailedcountryofbirthandnationalityanalysis/2013-05-16#:~:text=Passports%20held%20(nationality),which%20372%2C000%20were%20Irish%20passports).
4. https://www.ethnicity-facts-figures.service.gov.uk/culture-and-community/transport/driving-licences/latest#:~:text=The%20data%20shows%20that%3A,out%20of%20all%20ethnic%20groups
5. https://nordpass.com/most-common-passwords-list/
6. https://www.globenewswire.com/news-release/2022/08/02/2490352/0/en/Biometrics-Market-Size-worth-136-18-Billion-by-2031-CAGR-13-3-Notes-TMR-Study.html
7. https://www.gibsondunn.com/german-corporate-law-update-2023/
8. https://www.biometricupdate.com/202209/venture-capital-will-fund-biometrics-startups-based-on-founders-and-focus-over-product
9. https://www.w3.org/TR/vc-data-model/#:~:text=An%20assertion%20made%20about%20a%20subject.&text=A%20set%20of%20one%20or,can%20also%20be%20cryptographically%20verified.
10. https://www.ccc.de/en/updates/2022/chaos-computer-club-hackt-video-ident
11. https://www.linkedin.com/help/linkedin/answer/a1458457/id-verification-on-your-profile-with-clear?lang=en
12. https://fidodev.wpengine.com/new-research-reveals-consumer-frustrations-with-online-retail/
13. https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version/uk-digital-identity-and-attributes-trust-framework-beta-version
14. https://usa.visa.com/content/dam/VCOM/global/visa-everywhere/documents/visa-biometrics-payments-study.pdf
15. https://www.callsign.com/digital-trust-index
16. https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version

techUK
FOR WHAT COMES NEXT

About techUK

techUK is a membership organisation that brings together people, companies and organisations to realise the positive outcomes of what digital technology can achieve. We collaborate across business, Government and stakeholders to fulfil the potential of technology to deliver a stronger society and more sustainable future. By providing expertise and insight, we support our members, partners and stakeholders as they prepare the UK for what comes next in a constantly changing world.

linkedin.com/company/techuk

@techUK

youtube.com/user/techUKViews

info@techuk.org