The case for digital IDs

A techUK white paper | February 2019

Contents

Introduction

It is increasingly apparent in the UK, as we move into a digital world, where we shop, access services (public and private) and conduct financial transactions online, that a digital identity is becoming an essential requirement.

The need to repeatedly produce copies of physical documents to live our daily lives is anachronistic in the modern world. Moreover, the possibilities for fraud where online identification and authentication are not fully secure are proven by financial crime figures year on year.

The ability for individuals and businesses to use digital identities is key to unlocking value and facility of use for a wide range of services in both the public and private sectors. It will enable new services to be made available, secure against fraud, allow connectivity among digital services and greatly contribute to the economy as a whole.

In Appendix 1 of this Report we outline some of the numerous use-cases for digital identities and in Appendix 2 we list a number of Government databases, where, if permissioned access were available for verified digital identity operators, user experience and efficiency would greatly improve.

Given the technological expertise that exists in the UK, it is ideally placed to take a lead in this field, to develop strengths in digital identity, authentication techniques and standards and to export this homegrown expertise overseas. Online compliance and consistency with offline age verification regulations is also an important requirement for identity in the UK and globally.

Much progress has already been made, for example in the financial sector, as the UK and the City of London are global centres in financial services and security technologies. Within financial services, digital identification can be built on to move beyond KYC (know your customer) for consumers, to enable the streamlining of business to business services, which currently impose the costly burdens on industry involved in repetitive and wasteful due diligence. These additional trust services can position the UK as the global hub of digital trust and reinforce our dominance in global professional services.

Building on the strong security standards from the banking sector, standards can be reapplied to other sectors.

Banking security standards would satisfy Government departments which need to meet such standards themselves, such as Her Majesty's Revenue & Customs (HMRC) and the Department for Work and Pensions (DWP).

> **This paper will set out the position of the UK in relation to digital ID and online authentication, detailing the current situation and the needs of industry. It will argue that a coherent strategy is urgently required, with leadership and governance which can link up the public and the private sectors to enable strong, secure and trusted methods of digital identity to be widely available to citizens and to businesses.**

techUK’s recommendations for UK digital identity

1 Establish a Government policy to facilitate the creation of a fully functioning digital identity ecosystem, which operates across public and private sectors.

2 Nominate one point of contact within Government charged with leading this policy, in close collaboration with the private sector and full consultation with users.

3 Publicly release plans now for the future development of Gov.UK Verify, towards the creation of a framework of standards, which can be used by all players.

4 Provide plans for the further opening up of Government data (e.g. DVLA; HMPO; lost, stolen and fraudulently obtained documents, through services such as the Document Checking Service.)

5 Enable examinations, membership and utilities bodies to issue attributes digitally to enable thin file consumers to build up a track record of their activities: e.g. their qualifications, memberships, employment and paying customer status.

6 Recognise approved digital age and identity verification methods on an equal footing with paper based and face-to-face verification. Consistency is required in terms of online and offline.

7 Set up a new lawful basis for processing biometric data for identity verification and authentication in order to support legislation such as the Digital Economy Act and recognise that biometrics are being used to increase security and combat fraud.

8 Nominate a competent independent authority for digital identity.

9 Plans should be put in place for government-led communications to raise public awareness of the importance of digital identity.

Chapter one | The case for action

Everybody needs a way of proving their identity and authenticating themselves both in the physical and online worlds. The ways digital ID could improve the lives of citizens, businesses and other organisations, secure their data and facilitate their online activities are many:

Security and privacy	Managed properly, digital ID and strong authentication can provide security of data. Now that the exchange of data has become fundamental to a large part of economic activity and the General Data Protection Regulation (GDPR) has become UK law, it is essential that data be kept secure and that data subjects can be clearly identifiable where required (e.g. subject access requests under the Data Protection Act). When combined with multifactor identification such as device ID and biometrics, digital IDs become a secure method of verifying one's identity.
Maximise consent for users	A digital ID can enhance the ability of citizens to choose which data to share and better transparency on what their data is being used for.
Secure access to online financial services	A strong digital ID would promote the development of open banking and open services. The ability to log-on with one ID and access diverse accounts and product options (e.g. personal banking, pensions, mortgage, utilities, social security benefits) would greatly assist citizens in managing their finances and accessing products tailored to their needs.
Know your customer (KYC) and anti-money laundering (AML)	Financial institutions need to be able to establish the identity of individuals and businesses they deal with and, due to the critical importance and sensitivity of financial data, they must do so according to strong sector-specific, security standards. An ecosystem for digital identities could cut the costs of KYC by simplifying processes and reducing duplication.

Efficiencies for government services	Costs for social security benefits and pensions could be greatly reduced and efficiencies enhanced by the availability of digital IDs. Public services would also be easier to access and more personalised for citizens.
Proof of age	Individuals need to prove their age in various situations. The forthcoming Digital Economy Act sets out a range of age verification requirements, and an accreditation scheme is expected to be available shortly to help organisations needing to verify age online and in person. A range of privacy preserving techniques is ready for market - from tokenised sharing of an 18 plus attribute derived from a Government issued identity document, through to age estimation techniques.
Cross-border activity	Digital identity is becoming accepted in the international sphere as a way of ensuring greater collaboration across borders. It provides an opportunity to bolster international trade as well as combat fraud.

The plea from the technology industry

The plea from many in the tech industry is that the issue of identity needs to be joined up to tackle the need to manage multiple digital identities and consumer expectations on ease of access to all types of online service. Tech companies small and large are keen to assist and are coming up with solutions. But they are encountering hurdles in outdated legislation, the complexity of the regulatory landscape and in achieving recognition of their solutions in the market.

> **Recommendation one:** the UK Government should establish a policy to facilitate the creation of a fully functioning digital identity ecosystem, which operates across public and private sectors.

Of course, the Government has sole authority in defining and conferring citizenship and associated identity documentation. However, one in five of the UK population has no root anchor document, such as a passport or driving licence.[1] Also, there are a number of forms of identity in the UK, currently governed by a myriad of agencies and which, in a digital age, still operate on pre-digital lines.

- There are multiple Government departments for which identity is important to their operation, for example: Cabinet Office, Department of Culture, Media and Sport (DCMS), Home Office, Her Majesty's Passport office (HMPO), Foreign Office, Information Commissioner's Office (ICO), Driver and Vehicle Licensing Agency (DVLA), DWP and HMRC. In our view, the Government should nominate one single point of contact as lead on digital identity.
- There is increasing fragmentation across government departments, which are deploying different identity solutions, causing friction for user access.
- The UK currently has numerous different regulators and enforcers regarding identity, for example: British Board of Film Censors (BBFC) and Gambling Commission, Video Standards Council, the police, courts, trading standards bodies, local authorities.
- Identity solutions operate differently by sector (e.g. pharma, insurance, public sector) or they have been designed for particular uses (e.g. payments only, e-invoicing only or logistics).
- Solutions are defined by national boundaries and cannot operate cross-border.
- In a post-GDPR world, where data minimisation is a requirement, legislation, which requires physical copies of identity documents to be transferred and stored, should be reviewed and updated.

The current model of using passwords for online services is, as everyone knows, broken and instances of data hacking are soaring. We all hate passwords and they are not in any way secure. Nine in ten log-ins globally are bots trying to attack passwords through 'brute force' or using stolen surnames and passwords in thousands of websites to try to gain entry.[2] Digital identity presents an opportunity to promote strong and convenient authentication in place of weak and inconvenient authentication.

Parties which rely on solid proof of identity have certain basic requirements which can give them absolute certainty as to whom they are interacting with.

What is required is:

- interoperable standards;
- the ability to check/validate any identity;
- knowing and trusting the verifiers of identity;
- having an audit trail of who did what when;
- digital identities which are easy to set up and to use to facilitate widespread adoption.

> **In the view of techUK's members, there needs to be a solid UK strategy for digital identity, which consolidates input across all public bodies and departments as well as the private sector. If this is executed well, drawing upon the considerable technical know-how, which exists in the UK, it can protect citizens, reduce fraud and unlock value in the UK economy, driving both business and economic growth.**

Recommendation two: have one point of contact should be nominated within the Government as lead on digital identity.

Recommendation three: the Government should publicly release plans now for the future development of Gov.UK Verify, towards the creation of a framework of standards, which can be used by all players.

Recommendation four: the Government should provide further plans for the opening up of Government data (e.g. DVLA; HMPO; lost, stolen and fraudulently obtained documents, through services such as the Document Checking Service.)

Chapter two | Recent developments

Gov.UK Verify

On 9 October 2018, Oliver Dowden, the Minister for Implementation, made a statement, announcing the end of Government funding for the Verify scheme after a final 18-month contract for existing identity providers (IDPs). Two of the seven IDPs dropped out of the scheme, leaving five remaining - Experian, Post Office, Barclays, Digidentity and SecureIdentity. He noted that 'the Government expects that commercial organisations will create and reuse digital identities, and accelerate the creation of an interoperable digital identity market.'

This indicates a welcome shift in government thinking towards wider involvement of the private sector in the development of digital IDs. However, it was sparse on detail. What is to be done to progress matters during the remaining 18-month period? How exactly is the private sector to be involved? Is the intention to allow private organisations (subject to suitable controls) to access Government held databases on identity (e.g. passport and DVLA)?

Both guidance from the Joint Money Laundering Steering Group and the 'assurance levels' in the Electronic Identification and Trust Services regulation (eIDAS), which were adopted in the second Payment Services Directive (PSD2), state that being able to check data to positive databases is a factor in the reliability of an electronic ID. Therefore, the ability to make these checks will be necessary if private sector companies outside Verify are to be able to compete in this market.

> **The UK needs a detailed workable strategy through which the Verify scheme is to evolve into a standards-based ecosystem. The Government should set out a clear strategy for digital identity which will operate across the board: this is the only way to help both the public and private sector stay ahead of fraud and to allow UK citizens and companies to fully benefit from the digital world.**

Open Banking

Through online banking, many account holders use digital IDs to interact with their banks. The emergence of ‘challenger banks’ and digital only banking services has also led to the creation of new digital identities. Now, with the PSD2 and the Open Banking initiative, the number of digital identities in the financial sector, already in the millions, is bound to increase. It is essential that these identities are streamlined and standardised; otherwise fragmentation in this landscape will only increase.

Identity documents

Recently, the Home Office has outlined proposals to adopt leading digital identity technology, using the biometric chip read of passports remotely to enable 3.5 million EU citizens to prove their right to remain in the UK post Brexit.[3]

Given that the same technology approach would hugely benefit other areas of the economy, techUK hopes that Government is actively looking at extending this policy and supporting the use of digital identity verification more widely. This should enable individuals to:

- prove their right to reside and to work;
- be seen as acceptable for KYC checks;
- prove that they are over 18 to buy age restricted goods and services in the UK.

This may require the National Cyber Security Centre (NCSC) or other bodies to devise a suitably robust accreditation process. This should build on the work that the British Board of Film Censorship (BBFC) has undertaken for technology providers to meet the requirements of the Digital Economy Act.

Industry standards

As in many walks of life, digital identity will require standards to which all providers adhere and which are recognised by users, to ensure user protection, control, consent and good governance. This is particularly so in the financial sector where requirements are higher than in other areas. The British Standards Institution (BSI) brings companies together to develop standards, one form of which is the publicly available specification (PAS). This is a fast-track, UK standardisation specification, code of practice or guidelines, developed by sponsoring organisations to meet an immediate market need. It is not binding as such, but, if adhered to by the market, it can become an accepted industry standard.

Online authentication: On 18 September 2018, the BSI's Digital Identification and Authentication Code of Practice (PAS 499) was endorsed by the UK trade association for financial institutions, UKFinance. This deals with the requirements for 'strong authentication' and 'levels of assurance' contained in the PSD2, which apply to financial organisations. It covers customers creating and accessing their digital accounts; customers making a payment via a mobile device or other computer; customers making a contactless payment using an electronic device; a retailer receiving such payments; third-party access; delegated authority; and a bank or payment service provider administering such transactions. The endorsement of this PAS by the UK's financial sector heralds a streamlined approach to authentication and thus to digital IDs, which is to be welcomed.

Age verification: A second standard (PAS 1296), adopted in March this year, is a code of practice for the provision and use of online age checking services. It makes recommendations for an online framework that can be used, for example, to check the age of those:

- buying age-restricted merchandise online (e.g. e-liquids, adult materials, dangerous goods);
- accessing online content (e.g. streaming media, adult content);
- using online services (e.g. dating services, gaming or gambling websites); and
- accessing online age-gated material (e.g. education).

Chapter three | The way forward

What does a good digital identity scheme look like?

Innovation and competition will be fundamental to creating a digital identity framework that truly works for the public and businesses - one that is both efficient and cost effective. Any good digital ID will have to work for everyone and not just the technologically savvy. Further, consumers who currently have 'thin-files' (i.e. limited information in their credit history which hinders them achieving a good credit score) should be assisted through digital identity systems. This can be done through extended use of data available such as qualifications, memberships, employment and paying customer data.

Digital identities will also need to protect the privacy of citizens to ensure that their data is not misused or exploited. As such, a good digital identity framework will have both 'ethics by design' and 'privacy by design' at its core. It should be convenient, easy to use, have multiple adoption channels and be suitable for a range of ages, technological literacy and abilities. It will also need to provide

a) a long-term financial business model and
b) a functional solution which can continue to drive value over a period of time.

In addition, in order to be compatible with GDPR, good digital identities will have to support data minimisation - so that only the data necessary for the service is collected and where the citizen has control over access to their data. It would also be beneficial to support both anonymity and pseudonymity, given the developing requirements for access to online age verified services.

To make digital identity fit for purpose for consumers within both the public and private sector in 2019 in a post GDPR world, we need to build on the lessons learnt from organisations like the Privacy & Consumer Advisory Group PCAG, World Privacy Forum and Omidyar. The clear message is that the approach has to work for consumers; it has to be citizen centric.

In addition to robust technical security, consumers deserve transparency, customer redress, ethics and privacy principles by design. At present, there is no nominated body or standard which can address that breadth. Whilst there are several candidates, the UK does not have a clear technical review body that spans public and private sector for identity. In contrast the National Institute of Standards and Technology (NIST) performs this role ably in the US. In the UK, the Centre for Acceleration of Social Technology (CAST) or the National Cyber Security Centre (NCSC) could play this role with nominated audit bodies (for example, tScheme or one of the private sector audit bodies).

The points made above on the previous page lead us to:

> **Recommendation five: enable examinations, membership and utilities bodies to issue attributes digitally to enable thin file consumers to build up a track record of their activities: e.g. their qualifications, memberships, employment and paying customer status.**
>
> **Recommendation six: recognise approved digital age and identity verification methods on an equal footing with paper based and face-to-face verification. Consistency is required in terms of online and offline.**

What about liability?

There are differing schools of thought on liability models for digital identity. There are those who take the view that, given the current level of lost/stolen/fraudulent government-issued identities, a liability scheme for digital IDs is not feasible. There are others who regard a model for liability as being a basic requirement for the functioning of digital identity.

In this paper, we make no specific recommendation on liability, but outline the two differing views, which would require further examination and discussion.

View one: Liability framework is required

According to this view, a clear liability framework is important within any digital identity system, as with any multiparty arrangement. The roles and obligations of each party, and what happens in the event of failure need to be clearly defined and understood.

Federated digital identity schemes are based on a service provider (or relying party) trusting the attestation of an identity provider of the assurance of an identity. In this view, therefore, trust only exists if the service provider has confidence that the identity provider has fulfilled their obligations and that a failure to do so will have consequences – i.e. liability. An identity scheme may define this liability with variation on the party involved, the cause of failure, the impact of failure, the use case being enacted and the type of liability.

Liability would generally sit with the party responsible for setting processes or standards for identity assurance. This could be the identity provider, the identity scheme or an external agent. It is possible for each of these models to set liability at an uncapped amount, at zero, or somewhere in between.

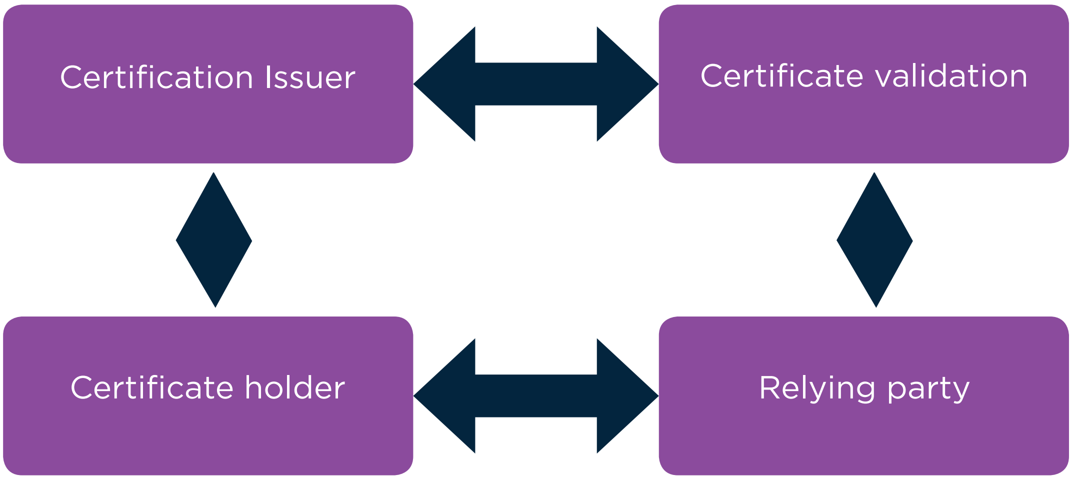
For regulatory liability in the financial sector, the fines imposed could be significant. If the bank could not back off this liability with the identity scheme it is unlikely that they would find a sound business basis for relying upon an identity assertion. For product liability, a failure of a party to perform their role and/or fulfil their obligations can be agreed; provided that both sides understand the level of liability, the scheme can operate effectively.

The trust model: One possible specific model proposes that liability for a multi-purpose digital identity solution should be a set of 'minimum operating rules', consisting of a trust model in the form of a set of contractual entitlements and obligations, which effectively provides a risk-mitigated assurance of identity. This model is very similar to the four-party scheme model, which has been in use for decades in the card payments sector. Such a scheme-based approach would provide rules for:

- common global standards (using established open standards);
- a global and scalable network, not dependent on multiple bilateral contracts;
- an application framework, which is open to all application providers.

These operating rules would rely upon 'thin' credentials, operated via regulated financial institutions. Emphasis would be on 'thin'- i.e. with no other attributes or entitlements at the identity layer, simply the attestation of identity by a person's financial institution according to recognised KYC procedures. What matters is how a person's attributes and entitlements are loaded onto that base platform, and that the individual has the choice as to when and where such attributes/entitlements are visible to a relying party. Such a digital identity would be backed up with a resilient pre-agreed liability model and a recognised dispute resolution process.

The model proposed can be represented as in the diagram below



View two: No liability framework

However, there is another school of thought, which sees liability as being both unnecessary and impossible in a competitive market for digital identity.

This view sees the currency of identity documents and attributes as very different to that of card service provision. In addition, the question remains as to who is liable if there is no means for a company to check against a Government Document Checking Service or access to lost and stolen databases to minimise fraud.

One of the challenges for the digital identity world is that root government-issued identity documents are known to be imperfect. There are fraudulently obtained genuine documents created in every country, known as FOGs. There are also lost and stolen documents. 174 countries contribute to the Interpol lost and stolen database which contains more than 68 million records.[4] There are also 'thin-file' individuals who do not have access to photo identity documents, but who may have mobile phone or utility data to start to build an activity history and there is likely to be a growing range of identity attributes. This is why it is not possible to adopt the same liability model for identity as has developed in the financial services card payments sector. It is important that governments open up access to the relevant database sources in controlled conditions to enable checking to source and against lost, stolen and fraudulent obtained genuine documents.

We therefore propose:

Recommendation 7: the UK should set up a new lawful basis for processing biometric data for identity verification and authentication in order to support legislation such as the Digital Economy Act and recognise that biometrics are being used to increase security and combat fraud.

Chapter four | The cost of not acting

Fraud

The steady shift of payments from face-to-face to online has seen a consequent shift in fraudulent activity. Increased digitisation has given rise to new forms of fraud, targeting many people and high value amounts. Spamming, phishing, identity theft, malware targeting individuals and cyber attacks against online retailers can allow fraudsters to obtain huge amounts of payment card data.

Changes in technologies and shopping habits have seen a shift towards online fraud and identity theft. In 2017, the UK's fraud prevention service Cifas reported 174,523 cases of identity fraud, a rise of 9 per cent on the previous year. 84 per cent of those frauds took place online.[5]

In March 2018, UK annual financial fraud figures showed an actual reduction in the total amount of fraud from £768m to £731m (2016 figures to 2017). Yet, fraud in online channels increased significantly over the same period, with

internet banking fraud increasing by	mobile banking fraud increasing by	e-commerce card fraud
19.3%	**10.5%**	**no reduction**

2018 has also seen analysis of a new category of fraud - the so-called authorised push payment (APP) scams - which at £236m dwarf the £37m reduction in like-for-like figures. APP scams involve individuals or businesses being tricked into authorising payments, which circumvent authentication security, and have led to 75 per cent of losses being borne by the victims, rather than the banks. Robust digital identity is critical to preventing this form of fraud from exploding, with some reports even suggesting that losses to SMEs could hit £13.5 billion.

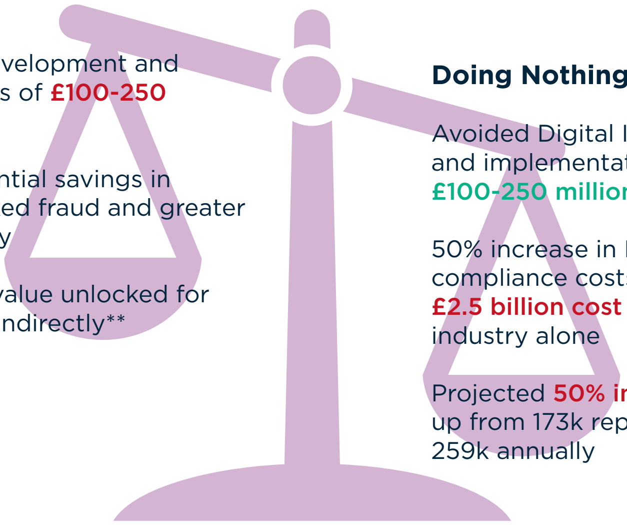
Lost ID documents and access

Currently, in their daily lives, UK citizens need to carry around physical documents, which are easily lost. Almost a million driving licences were lost by British drivers in the last year, according to latest figures released by the DVLA. British motorists applied for 931,527 driving licence replacements in 2017. Substitute licenses cost £20, meaning drivers forked out £18.6m on new ones.[6] The high cost of replacement begs the question as to whether there should be alternative approaches to issuing and relying upon such credentials. It is also worrying in terms of high volumes of documents potentially falling into the wrong hands.

In summary, if the current status quo of inaction in terms of digital identity persists, this could lead to a 50 per cent increase in cases of identity fraud by 2021 and an additional associated cost of £2.5 billion by 2021 to the banking industry alone.[7]

In addition, the separate nature of identity verification across national and local public services means that citizens must have multiple separate log-ins and passwords. A robust interoperable digital ID ecosystem would reduce friction and ease access for consumers.

The value of action vs inaction: 2021 projections



Doing Something

Digital ID scheme development and implementation costs of **£100-250 million***

£5-10 billion of potential savings in reduced identity-linked fraud and greater operational efficiency

Up to **£58 billion** in value unlocked for UK plc, directly and indirectly**

Doing Nothing

Avoided Digital ID scheme development and implementation costs of up to **£100-250 million**

50% increase in KYC and financial crime compliance costs - an **additional £2.5 billion cost** to the banking industry alone

Projected **50% increase in identity fraud** - up from 173k reported cases to 259k annually

* Based on scheme development costs elsewhere, and projected implementation costs across industries.

** Potential value creation includes digital identity as a catalyst to wider innovation in the digital economy.

The current UK public sector ID model

Unlike some other European jurisdictions, the UK has no ‘identity card’. It does, however, have the Gov.UK Verify scheme, which performs a function similar to many European ID cards in that it allows access to public services online.

Gov.UK Verify was first mooted in 2011. It was further developed by the Government Digital Service (GDS), part of the Cabinet Office tasked with leading the digital transformation of Government. Gov.UK Verify went live in May 2016. Citizens who wish to use the scheme are asked to choose one of a number of companies which will carry out the necessary identity checks to verify their identity. These companies - known as identity providers (IDPs) signed up through a tender process and were awarded contracts by the Department of Work and Pensions.

However, the current Gov.UK Verify scheme has not been used by citizens in the numbers envisaged and is costly for public sector organisations. Signing up is a difficult and lengthy process, involving knowledge-based questions to which many citizens will not know the answers.

The cost of setting up and running Gov.UK Verify has been considerable. As the existing Government contracts will cease in 2020, more transparency would assist in restoring public and business confidence.

Recognition of digital identities abroad

Any digital ID system, to be fully serviceable, should be useable within the citizen’s own country and also recognised by other countries. This was the aim of the EU in introducing a regulation on electronic identity and trust services in the single market in 2016 (commonly known as the eIDAS Regulation).

eIDAS covers trust services in general and the interoperability of government-recognised eIDs across the single market. It provides a mechanism for permitting and forcing acceptance of eIDs authorised by one EU member state in all other member states. Although eIDAS can only ensure digital ID recognition by public sector bodies in other member states, it does allow both public and private sector eIDs to benefit from such mutual recognition, e.g. the Italian private SPID scheme.[8] The procedure is by way of pre-notification of a scheme to the European Commission; peer-review by all member states and then full notification, after which cross-border recognition takes effect.

In August this year, the UK pre-notified Gov.UK Verify under the eIDAS scheme and the process of full notification is ongoing. However, it is not clear how the Government intends to proceed given the indications of changes to the scheme. Nor is it clear whether other commercial companies can notify in the UK now or in 18 months' time when the current Gov.UK Verify contracts end.

The UK therefore requires, as a matter of urgency a clear political drive towards the creation of a fully-functioning digital identity marketplace, which incorporates both public and private realms and which can be accepted for recognition in the EU and internationally. Such a drive should be coupled with a communications campaign to highlight the benefits of digital identities to the consumer. The long-term governance of a digital identity framework would, we suggest, be best managed through the establishment of a competent independent authority, or the allocation of this role to an existing authority.

Our final recommendations therefore are:

Recommendation eight: the Government should nominate a competent independent authority for digital identity.

Recommendation nine: plans should be put in place for government-led communications to raise public awareness of the importance of digital identity.

References

1. https://www.electoralcomm
2. http://info.shapesecurity.com/2017-Credential-Spill-Report-w.html
3. https://www.gov.uk/guidance/using-the-eu-exit-id-document-check-app
4. https://www.interpol.int/INTERPOL-expertise/Border-management/SLTD-Database
5. https://www.cifas.org.uk/secure/contentPORT/uploads/documents/External-Fraudscape%202018-Final.pdf
6. https://www.gov.uk/government/news/drivers-lose-almost-a-million-licences-in-the-last-year 2010 FOI request cites 303,881 lost/stolen (267,247 + 36,634)
7. Cost of doing nothing report table (Author Innovate Identity, Published Open Identity Exchange, April 2018)
8. https://ec.europa.eu/digital-single-market/en/news/first-private-sector-eid-scheme-pre-notified-italy-under-eidas

Appendix one: Use cases for digital identity:

Anti-money laundering:	Companies, in particular financial institutions and banks, are still asking consumers to either go to a physical branch to open an account or to post paper ID documents. Many companies are storing scans of full dates of birth and even full ID documents, rather than minimising the personal data stored. This is contributing to more 'honey pots' of data for hackers.
DBS disclosure & barring service or criminal record checks:	There are several routes for application, different documents and processes in each part of the UK. This is inefficient and expensive for Government, slow for individuals and organisations, creating problems with volunteers and staff hiring and mobility. Over 200,000 application forms per year are rejected due to input errors.
ID checks at bars and nightclubs:	Identity documents carrying a holographic mark or UV feature have to be carried physically and can therefore be lost or stolen. When IDs are scanned, there are concerns as to whether the quantity of data accessed is proportionate to meet the requirement of age verification and secondly as to how data protection guidelines are adhered to. Regulators have to avoid narrow legislation which rules out innovation, for instance for in store or online alcohol sales.
Name change via deed poll:	Although a free form is all you legally need to present to banks and other official institutions in order to confirm that you have changed your name, there is widespread confusion in local and central government about what constitutes an 'official' deed poll. For individuals the process is confusing, time consuming and can be expensive.
Right to work checks:	An employer or recruitment screener must train staff to review original acceptable documents, review face-to-face with the applicant and make a copy to keep on file with date of storage. This is expensive and inefficient for the both the recruiter and the applicant.
Right to rent checks:	A landlord or letting agent must see original acceptable docs, review prospective tenants face-to-face and make copies of documentation to keep on file with date of storage. This is expensive and inefficient for all parties, and carries significant risks around data protection. From a consumer standpoint it would be preferable to be able to transfer reference checks to different landlords and letting agents.

Age verification for access to age restricted content and purchases:

Young people under the required age are setting up accounts designed for those over 13 or over 18, by falsifying their age and/or creating a fictitious email account for parental consent. In many instances minimal checks are undertaken. There are clear social and health repercussions from underage access to alcohol, cigarettes and adult content. Grooming and trolling is prevalent on many gaming and social sites, which can have a knock-on impact on mental health, wellbeing, social & emotional development and educational performance.

Age verification for online gaming and quasi gambling:

Today online retailers of video games allow young people to self-assert their age when purchasing video games bearing a 12+, 15 + or 18+ classification. Likewise, there is no age verification on online games platforms. The PAS (Publicly Available Specification) 1296 for age checking presents a model for age verification for age-verified goods and services.

Age verification for access to public transport, sporting, leisure and community services:

The experience for young people as they first have to prove their age or identity in the local community to use transport services, take part in sporting activities or go to a cinema is not a smooth user experience.

Online reviews:

Millions of people look at online reviews and endorsements before making decisions such as where to stay on holiday, or which plumber to use. Using a digital identity would be a way for consumers to know that a real named individual has posted the review, even if the name is only known to the site.

Peer-to-peer meetings:

There are increasingly circumstances where people meet online first and then arrange to meet offline - such as online dating, online marketplaces, classified sites and sharing economy sites. This offers opportunities for the general public but also for fraudsters and criminals. In each of these instances an individual will be able to elect to share their digital identity and any additional self-selected attributes - e.g. over 18 and a watermarked photo to aid recognition when meeting up.

Voter registration, polling and e-voting:

Digital identity and facial recognition software can be used as a means of citizen verification for both voter registration, identification at polling stations, remote e-voting and polling.

Qualification screening checks:

For decades individuals have usually been presented with a paper certificate at the end of a course. Yet images of real certificates are widely available online for fraudsters to copy and then adopt as their own. A digital identity could be used to simply add existing qualifications or to sign up to a course, to verify the person taking coursework and sitting an exam. The qualification could be assigned to your digital identity and then easily shared with future employers, who in turn could trust the person has actually gained that qualification.

Title transfer:

The purchase of property is attractive for money laundering purposes. The UK is breaking new ground in terms of creating a public central register of beneficial ownership information. This could be enhanced by requiring biometric digital authentication and assigning a digital identity to the fixed paper deed assets being transferred. This could be expanded to share certificates and material contracts. Digital identity for assets can assist to control the asset ownership lifecycle.

UAV registration, ownership and licensing checks:

Today a person is required to register their competence to own a commercial unmanned aerial vehicle (UAV), i.e. a drone, in the UK. There is not as yet a commercial UAV register which matches ID checks to verify that the same person has undertaken the competency test, is of the required age, has purchased insurance and taken title of the drone. On an ongoing basis a biometric digital identity could check that the authorised person is at the controls. A medical and or DBS check may be required at a future juncture. These attributes could also be integrated to the biometric digital identity and be required in order to join the UAV register.

Utility bills or bank statements as a form of proof of address:

Consumers are today required to store and present paper copies of utility bills or bank statements to prove their address. This is a slow and tedious process for all concerned. It poses a cost in terms of paper and postage for businesses and the environment and a time and storage burden for consumers. A utility company or bank could provide an attribute to a consumer which states that they have been a customer for a certain time period.

Appendix two: public sector uses

There are a number of Government databases which, if permissioned access were available, then verified companies could request access to this data via an API that could offer a "Yes/No" response to confirm identity details.

This would simplify the process of verifying an individual's identity and streamline processes including right to work, employment screening and right to rent, whilst improving the user experience, reducing time, cost and fraud for all parties. The following are suggested databases, by no means exhaustive, which could help to corroborate facts about a person's claimed identity.

A	Armed Forces/Police/Fire Brigade/Ambulance Employer Registry
B	Bankruptcy/Insolvency Register
	Birth/Adoption registrations
C	County Court Judgments
D	DBS Basic or Enhanced Disclosure/Disclosure Scotland
	Death Registrations
	Deed poll or registry of name change
	Drone Ownership Register
	DVLA Register
E	Electoral Roll or Northern Ireland Voting Register
F	Firearms Register
	Freedom Card/60 + card Register
H	HM Prisons Register
	HMRC/DWP PAYE, Tax or self employment records
L	Land Registry Entry
	Lost and Stolen Documents Register (via Amberhill, Interpol, Europol)
M	Marriage Registry
	Mobile Network Operators
N	National Offender Management Service
	National pupil Database - or school enrolment records via LEA
	NI Number
P	PASS records
	Passport Register
	Professional qualifications bodies and institutes
Q	Qualifications bodies (GCSE, A Levels, Further/Higher Education Degrees and Diplomas...)
S	Security Industry Authority Register
	Social media site summary (e.g. Linkedin)
U	Utility companies (gas, electric, fixed line telephone, TV licence)

techUK represents the companies and technologies that are defining today the world that we will live in tomorrow.

Over 900 companies are members of techUK. Collectively they employ more than 700,000 people, about half of all tech sector jobs in the UK. These companies range from leading FTSE 100 companies to new innovative start-ups.

The majority of our members are small and medium sized businesses.

techUK.org | @techUK | #techUK