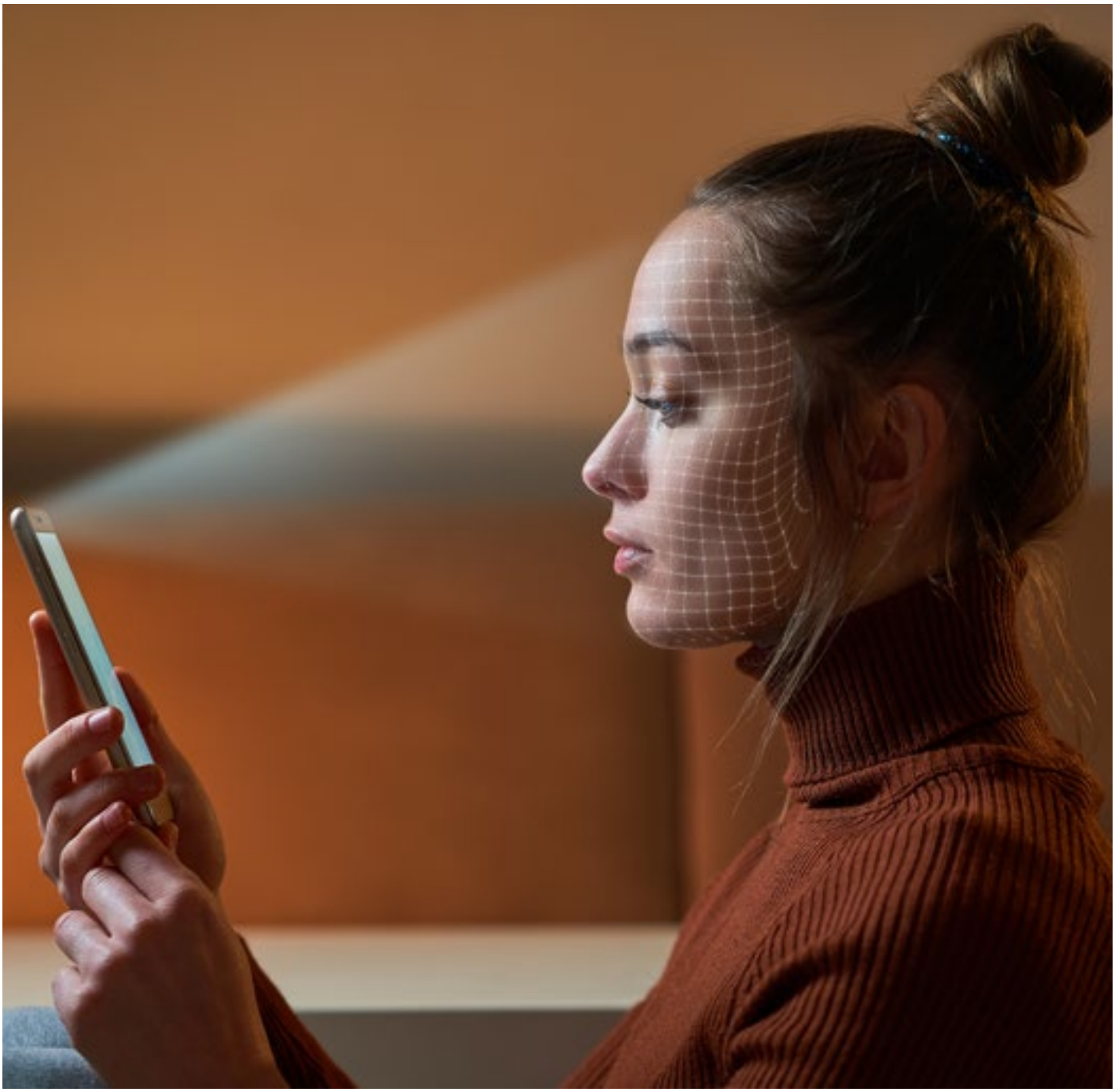
techUK

Digital identities: the missing link in a UK digital economy

A techUK white paper | August 2020



Contents

Our call to action

For too long digital identity has been the missing link in the UK's approach to digital policy making.

COVID-19 has made the need for safe and secure digital identity solutions even more urgent. The time to address this is now.

The Government must put digital identity at the heart of its forthcoming Digital Strategy.

Executive summary and recommendations

This paper follows on from the techUK White Paper of February 2019, 'The Case for Digital IDs'. Unfortunately, little progress has been made on the recommendations set out in that paper and, as we will show, the urgent need for digital identities has become even more apparent due to the COVID-19 crisis.

In this paper, we will reassess and revise our recommendations in the light of all that has and has not happened since February 2019. Chapter One will examine the clear and pressing need for digital identity thrown up by COVID-19. Chapter Two will detail the 2019 recommendations, analyse where action has been taken and explain the clear need for government to catalyse this market. Chapter Three will examine the current developments in the provision of identities into the public sector and what more is required. Throughout, we set out our vision for digital identities in the world into which we are emerging after the COVID-19 crisis, and explain techUK's new set of recommendations, summarised below.

Digital identity has a long history in this country, yet UK citizens still do not have widespread access to digital identity services. COVID-19 has shown how difficult this makes conducting day-to-day activities in a digital way. Such services are now absolutely essential for consumers: they give security of personal data, protect against online fraud, embed data-minimisation and allow individuals to apply for jobs, obtain housing and conduct financial transactions in a fully digital way.

Digital identities also allow citizens to control where their data is shared and to what purpose it is put, tools which combat any potential unethical uses of data.

However, in recent years, government has focused on digital identity in the public sector, from the perspective of government as a user of digital identities. What is needed, however is a market for digital identities, which spans public and private sector in an interoperable way. Yet in markets which are networked; where multiple parties are involved; where interoperability and mutually respected standards are key, the private sector is not always able to act alone: it needs a centralised catalyst, a convenor, to promote, and indeed to pursue, collaboration amongst competing players.

As we emerge from the COVID-19 crisis, government must take a lead in digital identity as an essential tool for the whole digital economy, not just for the smooth functioning of digital government. It must step beyond its own parameters and play a proactive role in enabling all citizens to have access to a functioning digital identity market. This is, after all, how digital identity has come to fruition in most other major jurisdictions.

The UK has been trying to establish digital identities for over 20 years: it has not yet succeeded. What more does the government need to persuade it that its current stance is not working and that a new strategy is urgently needed?

techUK recommends:

When it comes to digital identity, the UK needs three things:

- A functioning market for digital identities, which can be used in the private sector. For this to happen, government must take the lead.
- Real competition in the market for the provision of identity services into the public sector.
- Thirdly, UK citizens need to be able to use the same identity whether they are dealing with private or public sector aspects of their lives.

We set out on the next page a list of recommended steps to these ends.

1. Government as enabler of digital identity market.

1. Put digital identity at the heart of the upcoming Digital Strategy and the Data Strategy.

2. Publish, as a matter of urgency, the response to the Call for Evidence on digital identity, to include coherent policy statements on:

(i) how the provision of digital identity services into government is to be opened up to competition (this should not only be standards documents);
(ii) Government action to catalyse the private sector market.

3. Ensure all legislation, which stands in the way of digital identities, is revised to recognise that digital/electronic identification and digital identity are acceptable and preferable in all instances (for a list of the main statutes, see Appendix 1).

4. Accelerate work to allow private sector providers access to scalable interfaces into government databases (e.g. HMPO, DVLA).

5. Foster the creation of an oversight body made up of public sector and private sector experts with the remit:

(i) connect identity initiatives across the economy, embedding consumer-first principles;
(ii) ensure security and reliability standards are met;
(iii) foster public trust through trustmark/certification;
(iv) oversee the implementation of ethical rules on data use.

6. Work in collaboration with international governments, non-government organisations (NGOs) and standards bodies to enable interoperability of digital identities internationally.

2. Government as consumer of digital identities:

7. Ensure that the provision of digital identities into the public sector is opened up to real competition, by updating government standards to align with the technologies and capabilities currently used in the private sector.

8. Complete as a matter of urgency, the Trust Framework and pilot scheme to enable private sector companies to provide digital identities into public sector/ local government as soon as feasible.

9. Ensure that the future Trust Framework is interoperable with the EU, by making it the UK's new notified scheme.

Chapter one: Life after lock-down

While the need for the UK economy to utilise the benefits of digital identities has been patent for some time, the Covid-19 crisis has very clearly evidenced the deficiencies of current manual/face-to-face identity checks. Some public bodies have taken ad-hoc measures to deal with the pressing and urgent needs, which could not be solved through conventional identity tools. But these short-term solutions, which are piecemeal, without reference to coherence or interoperability cannot be allowed to persist. Now is the time to take the reins and establish a coherent strategy for the provision of a well-functioning digital identity market.

The effects on the economy

The UK, and the world, will suffer a period of severe economic recession as a result of this pandemic. The OECD has estimated that globally, the loss of income could exceed that of any previous recession over the last 100 years and that the UK could face an 11.5% drop in GDP[1]. Unemployment is soaring and inequality has been exacerbated.

The Government provided an impressive package of economic support during the crisis and is continuing aid to restart the economy. We applaud this. However, access to digital identity services could play a significant enabling role in the recovery, in an environment where social distancing and contact tracing are likely to remain necessary for the foreseeable future. Expert studies show that digital identities could deliver very significant economic benefit. A pre-Covid report by McKinsey[2] estimates that digital identity could increase UK GDP by as much as 3% by 2030. Figures from the Open Identity Exchange (OIX) estimate that savings to the UK economy due to fraud-related savings could be circa £10 billion (£8.5Bn fraud/£1.5Bn in KYC operational savings), whilst the wider benefits to the economy could be closer to £60 billion.

In the UK's recovery from this crisis, secure and trusted digital identities will be key to allow us all to function in the more digitally-focused world into which we will emerge.

Ways digital identity will support the recovery

In continuing to battle the virus:

- **Contact-tracing:** On 4 July pubs and restaurants re-opened in the UK, with the guidance that customers should be asked to leave their names and phone numbers on a paper list at the door for contract-tracing if required. Irrespective of the doubts as to compliance with the GDPR, this system is hugely inefficient and unreliable. Digital identity would solve this problem and would lift some of the burden on hospitality and other service sectors.

- **Immunity certificates:** for some time to come, we will have to rely on testing for the virus and for antibodies. If it is established that the presence of antibodies confers significant immunity to Covid-19, then immunity certificates could be added to a digital ID.

In aiding the economic recovery:

- **Job seeking and recruitment:** Covid-19 has closed businesses and put many thousands out of work. People need to be able to apply remotely for jobs, which can only be done through secure, digital identity verification.

- **Right to work and Disclosure and Barring Service (DBS) checks:** Similarly, these necessary checks to assure the identity and the reliability of workers and volunteers can be done far more quickly and efficiently through digital means.

- **Benefits and government assistance:** The need for swift and efficient processing of applications for social security and government assistance schemes has never been higher. Both individuals and SMEs would hugely benefit if they could digitally prove their identity and, through this identity, coupled with open banking, enable checks to be made on their eligibility.

- **Inclusion:** the social exclusion resulting from Covid-19 is a major issue, which must be tackled. Digital ID allows people who do not have traditional ID documents to prove their identity using other attributes.

- **Retail:** The burden on retail staff in checking physical identities when selling alcohol and age-restricted products is inefficient and can leave staff facing aggression or violence. Being able to perform digital age verification would save valuable staff time and remove any possible dangers.

- **SMEs:** Many SMEs are struggling to find a way to operate safely and efficiently in a remote-first world. They urgently need corporate identity solutions to streamline the onboarding and verification process, one which works for both the party proving the identity, as well as the verifying party. techUK members have developed solutions which save time, money, and the requirement to meet in person, while strengthening the certainty and security of both the KYC process as well as follow-up interactions such as confirming client instructions.

- **Property transactions:** Identity is crucial in property transactions, but to allow this major market to operate without face-to-face interaction, digital identity will be key. Indeed, the Law Society, the Council for Licensed Conveyancers (CLC) and the Chartered Institute for Legal Executives (CILEx) have recently joined together to examine using digital identity in conveyancing.[3] Without a broad, economy-wide ID strategy, however, such initiatives will undoubtedly result in a highly fragmented market.

These are no doubt just some of the instances where digital identity would hugely benefit the economic recovery – and future of the UK. We cannot be complacent at this time and fall back on solutions that 'make do and mend'. The UK must wholeheartedly invest in the digital economy to come, by laying strong and long-lasting foundations.

On 23 June, Digital Secretary, Oliver Dowden, announced that in the autumn, the government will publish a new Digital Strategy to reflect the post COVID-19 reality.[4] The word 'identity' was not mentioned. Similarly, a new Data Strategy is to be unveiled. In our view, the post COVID-19 world will be one where the way people work, seek employment, conduct their business and personal lives will see a permanent change. Many systems will shift to, and remain, digital as a result of the needs this virus has imposed. Our opportunity is to put in place a connected data-led digital economy, where data is used and re-used multiple times in new and innovative ways by many players in the economic ecosystem. Crucial to such an economy will be consumer trust in the safety of their data and consent in the use of it for specific purposes. In our view, this trust can only be secured if citizens can safeguard their data and access their online worlds through the use of digital identities.

Secure and reliable digital identities will be a key requirement in this world. The applicability of the speed, simplicity and efficiency of digital identities in a post-COVID-19 world is absolutely clear. The significant cost savings and swifter procedures for individuals, private businesses and the public sector are easily apparent.

This is why digital identity must be a major element of the Digital Strategy and Data Strategy.

> **techUK recommends: the Government puts digital ID at the heart of the Digital Strategy and the Data Strategy.**

Chapter two: Government as an enabler of digital identity

Recent developments

Successive governments in the UK have struggled with digital identity for over 20 years, even though the potential benefits have long been recognised. As early as 2008, a report from James Crosby, 'Challenges and opportunities in identity assurance' noted:[5]

> "those countries with the most effective ID assurance systems and infrastructure will enjoy economic and social advantage, and those without will miss an opportunity... The ease and confidence with which individuals can assert their identity improves economic efficiency and social cohesion, which in turn leads to a greater number of transactions being reliant on such ID systems, further enhancing delivery of economic and social goals."

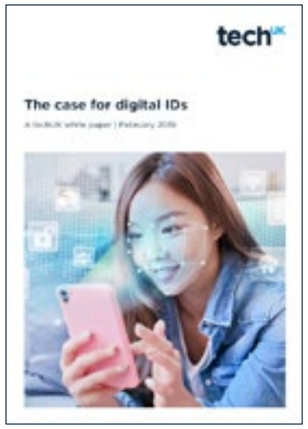
Since this time, we have had a series of initiatives, which have not achieved the desired result of citizen-friendly identity system. Instead they have failed and/or missed their target, while drawing heavily on the public purse. It is time now for the UK to reap the benefits of these intentions. We have been waiting too long.

From mid-2018, techUK took the view that Government action was absolutely required to coordinate the creation of a digital identity market. We understood that a common framework and standards with an agreed governance system was the best way to establish an interoperable system.

techUK White Paper 2019

In February 2019, techUK published a paper, which set out nine recommendations on what Government needed to do to assist in the establishment of a digital identity market in the UK.

The table on the next page lists these recommendations and below each, notes the response from Government, in particular the Government Digital Service (GDS) and the Department for Culture, Media and Sport (DCMS).



It is clear that the delays caused by Brexit and the absolute necessity of addressing the COVID-19 crisis has prevented Government action across the board. Yet it is highly discouraging that out of nine recommendations, only four have been partially addressed and, on the remaining five, not only has no action been taken, but no communications have been made as to the Government's intentions.

1	Establish a Government policy to facilitate the creation of a fully functioning digital identity ecosystem, which operates across public and private sectors. **GDS has been working on a Trust Framework of standards for digital ID, releasing drafts to a limited number of stakeholders. This process is slow and opaque (see p11).**
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. **The Digital Identity Unit, to be staffed from DCMS and GDS, was announced in 2019. However, since then, there has been no publicly communicated announcement on the scope of its remit, its resources, who will lead it or what powers it will have.**
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. **GDS has been working on a Trust Framework of standards for digital ID, releasing drafts to a limited number of stakeholders. This process is slow and opaque (see p11).**
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.) **A DCMS pilot was announced in 2019, which would allow selected private firms access to HPMO data only. The tender process was completed and the pilot began in April 2020, as we understand it, for one company at a time. Progress on this is much too slow.**
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. **No Government action.**
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. **No Government action.**
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. **No Government action.**
8	Nominate a competent independent authority for digital identity. **No Government action.**
9	Plans should be put in place for government-led communications to raise public awareness of the importance of digital identity. **No Government action.**

Further techUK action

Following publication of our 2019 White Paper, techUK made strenuous efforts to collaborate with government and stakeholders towards identifying measures needed to create a digital identity market which would span both public and private sectors.

We formed a set of working groups, together with Open Identity Exchange to look at:

(i) architectural interoperability;
(ii) inclusion;
(iii) liability and trust and
(iv) interoperability and standards.

Both GDS and DCMS were members of the Steering Board of these working groups. The groups made detailed analyses and reported back with detailed technical recommendations in February 2020.

In addition, we, along with a record number of UK companies and stakeholders responded to the Call for Evidence on Digital Identity issued by DCMS in July 2019 and closed for contributions in Sept 2019. Despite numerous assurances, no response to the Call for Evidence or follow-up steps has been released.

Instead, government is still focusing on the provision of identities into the public sector (see Chapter Three) but is leaving private sector to sort the problems out itself. In our view, this will not work for digital ID because:

- This is a two-sided collaborative market, which involves providers and relying parties both operating on an agreed set of rules.
- Different sectors have different levels of requirements.
- Standards are required to enable interoperability.
- Digital identity is not an end in itself – it is a tool which enables the flow of data in a digital economy and therefore new and innovative services.

In the light of all these factors, the private sector has not been able to deliver digital identity. If it had, it would have done so by now. Just as open banking would not have happened without the order from the Competition and Markets Authority, digital identity, will struggle without Government action and the UK will lag behind the rest of the world in the transition to a digital economy.

What we need now

Removal of legislative barriers

In addition to the above, there are pieces of legislation still on the statute book, which mandate the use of face-to-face identification and the checking of paper documentation. This is simply no longer necessary or appropriate in a world where much of our daily business is conducted online and where removing such mandates can have huge savings in terms of cost, efficiency and the protection of health from disease. The digitisation of existing face-to-face checks should be seen as a precursor to implementing digital identity. (A list of the main legislative barriers appears in Appendix 1.)

> **techUK recommends that the government ensures all legislation which stands in the way of digital ID is revised to recognise that digital/electronic identification and digital identity are acceptable in all instances.**

Access to government databases

An identity must be authenticated at each point where it is relied upon and therefore private sector identity providers need to be able to securely check public databases such as those for passports and driving licences. The document checking service pilot scheme, currently running to eventually enable this, is proceeding at a very slow pace. It should be expanded and accelerated with the end goal of providing truly scalable digital services via modern APIs. Security and trust can be enabled by requiring API consumers to be regulated or certified organisations.

> **techUK recommends the acceleration of activity to allow private sector providers access to scalable interfaces into government databases (e.g. HMPO, DVLA).**

True public-private sector collaboration

In our view, what is required is true public-private collaboration. Other nations have made great strides in creating world-class digital identity schemes and the noticeable difference is in how those governments have truly worked with the private sector. For example, in Belgium, the government took the lead from the private sector and integrated solutions developed by the banks and telcos[6] and in Canada progress has been made through coordinated and determined collaborative work.[7]

In our view, what is needed is for government to openly work with the tech sector to solve problems – as has been done in Estonia. In numerous jurisdictions, governments have sponsored or engaged with hackathons to address issues raised by COVID-19.[8] This is the kind of collaborative thinking we need to see in the UK.

Local government also needs to be empowered to embrace digital transformation across a citizen's lifetime. Too many local government solutions in the UK still rely on outdated manual processes: help from the private sector should be actively sought to find routes to digitalise local systems.

Consumer trust

An essential element of any identity system is trust: the public must have the assurance that whatever identity system they choose is legitimate, secure and trustworthy. If the government were truly willing to collaborate with the private sector to establish industry-wide standards, digital identity is far more likely to command the trust of the population and mitigate legitimate concern over the ethical use of data.

We need to build consumer trust and confidence in digital identity and the force for good that it can be. This should focus on the benefits of digital identity such as:

- **Enhanced privacy:** digital identities can be built using principles of data minimisation, therefore giving consumers greater control of their own data privacy.
- **Enhanced security:** digital identities are very effective in fraud prevention by reducing the possibility of hacking and impersonation when accounts are accessed subsequent to onboarding.
- **Economic benefit:** reducing the transaction costs of the ecosystem, preventing otherwise increasing and costly identity fraud and creating more frictionless engagements with a whole range of societal interactions via both public and private sector service delivery.

- **Reduced financial exclusion:** providing legal identity to the under-banked and financially excluded, enabling them to access a whole range of public and private services with a trusted identity.
- **Enable people to connect with their communities:** smart cities offer a future in which citizens will not only connect with central services, but also engage with their local communities in ever more creative ways. Digital identity is a clear enabler for ensuring citizens can access the benefits of smart cities seamlessly and securely. This will deliver economic benefits, including significant efficiencies across local government.

In the light of the above, **techUK recommends that the government:**

- **Publish, as a matter of urgency, the response to the Call for Evidence on Digital ID, to include coherent policy statements on:**
  - **how the provision of digital identity services into government is to be opened up to competition (this should not only be standards documents);**
  - **Government action to catalyse the private sector market.**

'Digital ID can also unlock noneconomic value, potentially furthering progress toward ideals that cannot be captured through quantitative analysis, including those of inclusion, rights protection, and transparency. Digital ID can promote increased and more inclusive access to education, healthcare, and labour markets; can aid safe migration; and can contribute to greater levels of civic participation.'

McKinsey, Digital Identification, a key to inclusive growth, 2019

- **Foster the creation of an oversight body made up of public sector and private sector experts, which would act as a 'Digital Identity Implementation Committee' for organisations investing in actively delivering solutions:**
  - **Connect identity initiatives across the economy, embedding consumer-first principles**
  - **Ensure security and reliability standards are met**
  - **Foster public trust through trustmark/certification**
  - **Oversee the implementation of ethical rules on data use**

International standards

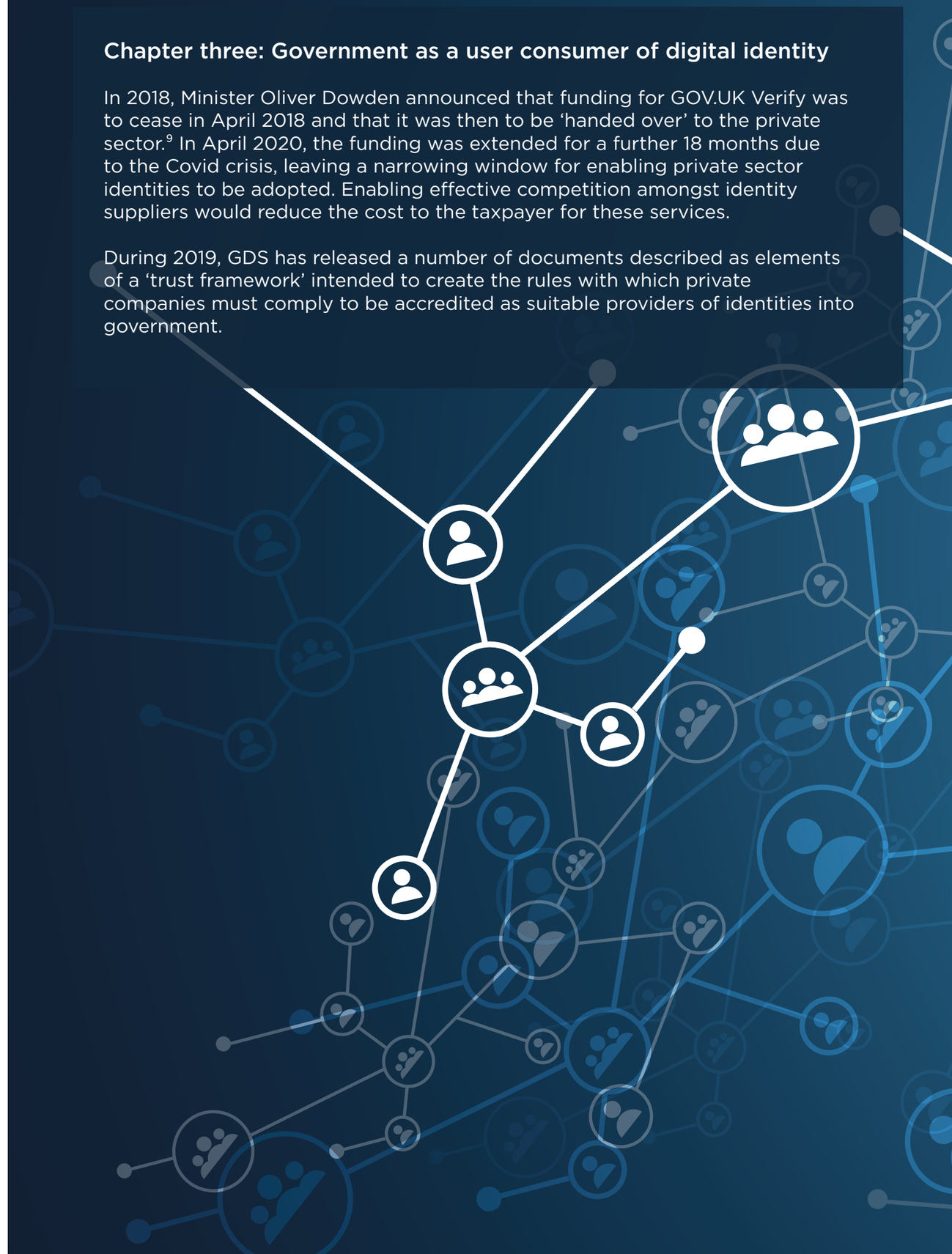
Identity is not just a national concept: people need to travel, transact and conduct business abroad and therefore any national identity must be recognized overseas. The World Economic Forum is currently running a working group looking at the principles which are key to identity with a view to defining and documenting common requirements. We urge that collaboration on standards should be as international as possible:

> **techUK recommends: the Government work in collaboration with international governments, non-government organisations (NGOs) and standards bodies to enable interoperability of digital identities internationally.**

Chapter three: Government as a user consumer of digital identity

In 2018, Minister Oliver Dowden announced that funding for GOV.UK Verify was to cease in April 2018 and that it was then to be 'handed over' to the private sector.[9] In April 2020, the funding was extended for a further 18 months due to the Covid crisis, leaving a narrowing window for enabling private sector identities to be adopted. Enabling effective competition amongst identity suppliers would reduce the cost to the taxpayer for these services.

During 2019, GDS has released a number of documents described as elements of a 'trust framework' intended to create the rules with which private companies must comply to be accredited as suitable providers of identities into government.



There are numerous issues with the process by which this is being done:

- The 'Framework' is to have 33 documents in it, but each is being released separately and companies are expected to comment with no knowledge of what will be in the rest of the documentation.
- Only a small number of companies are being consulted.
- The process is unacceptably slow.
- Very little information has been released on the overall intention of government concerning digital identity as a tool for digital growth.

But by far the most troublesome issue is that the standards themselves do not correspond with the technical capabilities which exist in the private sector. In practice, potential providers would have to 'down-grade' their technologies, modify their privacy-by-design principles and take a step back to provide solutions which comply with these standards. This cannot be acceptable or desirable. Government standards should be:

- technology agnostic;
- pitched at a high enough level that providers can comply using the most up to date technologies;
- flexible enough to allow for innovation;
- privacy-centric.

The outcome we foresee is very worrying. Small, innovative suppliers will not be able to wait a year and a half to be able to apply to provide identities into the public sector: they will go to other countries. Nor would it be economically viable for them to adjust their technologies to fit anachronistic standards. In the end, the UK will be left with just one or two providers willing and economically able to supply these services (as is the situation at present). This is not the way to create a competitive market.

techUK recommends that the government:

- **Ensure that the provision of digital ID into the public sector is opened up to real competition, by updating Government standards to align with the technologies and capabilities currently used in the private sector.**
- **Complete Trust Framework and pilot scheme to enable private sector companies to provide identities into public sector/ local government by autumn 2021.**
- **Ensure that the future trust framework is interoperable with the EU, by making it the UK's new notified scheme.**

Chapter four: Summary and conclusions

Government action is required

There can be no question now as to the need for digital identity in the UK. Yet, if the private sector resorts to establishing, piecemeal, systems, which operate in disparate spheres, this would raise a number of problems:

- **Fragmentation:** It would produce fragmented solutions, which operate in different sectors but do not interoperate.
- **Standards:** Different standards could be developed for different areas with no common basis.
- **Trust:** Private sector digital identity solutions, which have no 'sanction' from a centralised authority, (by way of a trustmark, certification or conformity with approved standards) tend to be less trusted by the public and also by potential relying parties. Establishing a place in the market and growing to scale are therefore problematic.
- **Data-flow:** A different set of systems for accessing the private and the public realm could hinder the freer-flow of information necessary in a digital world.
- **Public sector:** It would not solve the pressing needs of many government departments.

In our view, it is therefore not an option for the government to continue to insist that it sees no need to collaborate with the private sector in establishing an interoperable public/private sector digital identity market. It is also not tenable to propose that technologically advanced private players should comply with standards which do not allow for innovative technological solutions (see chapter three).

The emergency measures necessitated by COVID-19 have forced a mass use of digital technologies across all spheres, hitherto unseen. They have also possibly plunged us into the worst economic recession, according to some figures, since the Great Depression.

'Capturing the value of good digital ID is by no means certain or automatic. Careful system design and well-considered government policies are needed to promote adoption and manage associated risks.'

McKinsey, Digital Identification, a key to inclusive growth, 2019

If the UK is to emerge from this, we must use the lessons learned and take difficult decision. Now is the time to refresh our economy from the roots and embed digital ways of operation into its very fabric. This, we hope, will be the thrust of the Digital Strategy and the Data Strategy promised for autumn 2020.

Our identity is at the heart of all we do in our daily and business lives: the ability to prove it digitally must be a central plank of this rebuilt digital economy. Now is the time for the Government to grasp the nettle, throw out old unsuitable systems and ideas and embrace the imperative of digital identity.

Appendix one

List of most significant legislation and guidance to be revised:

- Immigration Act, 2014 and the associated government guidance on the 'Right to rent', which places duties on landlords to check physical identity documents.
- Immigration, Asylum and Nationality Act 2006 and associated Government guidance on the Right to Work. The guidance in relation to which places duties on employers to check physical identity documents.
- Power of Attorney Act 1971 as amended by Law of Property (Miscellaneous Provisions) Act 1989.
- Licensing Act 2003 (Mandatory Licensing Conditions) (Amendment) Order 2014. This prevents digital identity being used to demonstrate proof of age for the purchase of alcohol. (A proposed Amendment 52 to the Business Planning Bill 2019 - 21 would allow for the use of digital age verification.)
- Law of Property (Miscellaneous Provisions) Act 1989, section 1.This sets up the rules for witnessing, requiring that a witness is 'in the presence' of the signatory. As interpreted by the Law Commission, it prevents digital identity from being used for remote witnessing.

References

1. https://www.oecd.org/coronavirus/en/
2. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
3. https://hmlandregistry.blog.gov.uk/2020/05/29/facing-up-to-the-digital-identity-challenge/
4. https://www.gov.uk/government/speeches/digital-secretarys-closing-speech-to-the-uk-tech-cluster-group
5. https://www.statewatch.org/media/documents/news/2008/mar/uk-nat-identity-crosby-report.pdf
6. https://www.europeanpaymentscouncil.eu/news-insights/insight/discover-itsmer-belgian-digital-id
7. https://diacc.ca/
8. https://www.forbes.com/sites/tomokoyokoi/2020/06/10/beyond-the-covid-19-hackathons-matchathons/
9. https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2018-10-09/HCWS978/

techUK

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