techUK
FOR WHAT COMES NEXT

Unlocking UK Digital Identity in 2022

June 2022

Contents

Executive summary

In techUK's 2020 White Paper on Digital ID, 'Digital Identities: the missing link in a UK digital economy'[1] we called for action to develop "a market for digital identities, which spans public and private sector in an interoperable way".

Since that report was published, we have seen progress made towards the creation of a fully functioning Digital ID marketplace by the UK Government with the publication by DCMS of the Alpha version 2 of the UK Digital Identity & Attributes Trust Framework[2] in September 2021 following a lengthy period of consultation with - and substantive input from - the Digital ID industry and other key stakeholders. Crucially, this included the proposed creation of a governing body to oversee the Framework, to set up an accreditation and certification process for ISPs (Identity Service Providers) monitor compliance, manage enforcement, complaints and redress, collaborate with other stakeholders (both domestically and internationally) and both promote and encourage inclusion.[3]

In March 2022 the DCMS' Digital Identity & Attributes Consultation Response[4] went further, outlining a governance structure with a '…principles-based approach to digital identities and attributes[5]…' and the legislative changes necessary to support it. Additionally, following the Queen's Speech on 10 May 2022, DCMS have also confirmed that the legislation required to deliver their objectives as outlined in the Consultation Response will have space made for it as part of a data reform bill during the current 2022/23 parliamentary session.

Whilst these are welcome developments, now is not the time for complacency or slowing down. Far from it.

Greater action is still required and urgently needed.

That the UK is, upon publication of this report, still lacking a firm plan and timetable for the creation of the proposed new governing body within DCMS (OfDIA) and remaining issues regarding the wording of the UK Trust Framework that affect the ability of companies certified under the Framework to perform necessary KYC and anti-fraud checks as they do today under existing Data Protection Act 2018 and UK GDPR is cause for concern. Without greater clarity and certainty on these and other outstanding issues with the Alpha Trust Framework itself, the UK will find itself significantly behind other leading nations around the world who have not been slow to recognise the fundamental importance of Digital ID to their economies and who are moving swiftly to implement properly regulated ecosystems that will allow it to flourish.

techUK believes that the development of a thriving digital economy is firmly predicated upon the creation of a secure, flexible, and fully interoperable Digital ID ecosystem. But as an industry, we are still missing the clarity that only proper market regulation, allowing full interoperability, privacy by design, inclusion and transparency can deliver.

This report outlines ten key recommendations where action is needed urgently to enable the rapid creation of the effectively regulated market that industry believes is required. These are;

1. DCMS to create a formalised timetable to enable the full implementation of the UK Digital ID and Attributes Trust Framework during the first half of 2023
2. As DCMS have recently indicated, the associated legislative changes required to support the UK Trust Framework should be timetabled during the 2022/23 parliamentary session
3. GDS's One Login for Government platform build should be fully opened to competition and tender process
4. Certified ISPs should be granted access to government department-owned data attributes/credentials under the proposed 'Legal Gateway' during the first half of 2023
5. The creation of a permanent Public/Private Governing Body which owns, defines, promotes, and certifies against the Trust Framework during the first half of 2023
6. Government to allow full interoperability between Public & Private Sector Digital IDs
7. A detailed plan and timetable to create a unique, independent UK Regulator to oversee UK Digital ID ecosystem by the end of 2023
8. Government proposals on the future of the UK Data Protection Act must provide more clarity to UK ISPs on areas that may impact the use of Digital ID in the UK
9. Public engagement to build public trust and confidence in Digital ID must be prioritised by Government Communications Service and a plan put in place for 2023
10. DCMS and industry stakeholders to create a formalised joint working group to co-operate and accelerate delivery of the UK Trust Framework during 2023

techUK calls on the UK Government to create a detailed and meaningful timetable to address these remaining challenges and to bring its power to bear to deliver the legislative changes required to fully implement the UK Trust Framework during the current 2022/23 parliamentary session.

Introduction

In 2020 techUK published its second Digital ID White Paper, 'Digital Identities: the missing link in a UK digital economy'. In that report, we made the case for Digital ID as the key to unlocking the economic and societal potential inherent in a thriving UK digital economy.

We highlighted the opportunity for the UK to develop a vibrant Digital ID market, and the steps required by Government to make this happen. However, we stressed that this would only happen if further significant action was taken to create a robust, yet flexible regulatory and legislative structure that encouraged both technical and commercial innovation in the sector as well as full interoperability between schemes across both Public and Private sectors.

We called for closer, co-ordinated, and transparent co-operation between the UK Government and the Private Sector to enable the creation of a fully interoperable, secure and user-friendly Digital ID ecosystem, allowing UK Citizens and businesses to engage and transact online safely and securely.

If we are to get Digital ID right for the UK, we stressed that the UK needed three things:

1. A functioning market for digital identities, which can be used in both the Private and Public Sectors. For this to happen, Government must take the lead

2. Real competition in the provision of identity services into the Public Sector

3. UK Citizens to be able to use the same identity whether they are dealing with private or Public Sector aspects of their lives

A dramatic and eventful two years have now passed. We have experienced a global pandemic, a correspondingly steep increase in the levels of consumers transacting online and a sea change in consumer buying behaviours away from physical retail into online. Where physical interactions were not possible because of the pandemic, the power of digital technologies, including Digital ID, has been centre stage in keeping us all digitally connected whilst being physically apart.

As an example, we saw a number of Government-related services allowing digital identities to be used in lieu of physical documentation, most notably in the NHS Login and the Home Office's EU Settlement Scheme/EU Exit Apps both of which featured facial biometrics as an integral part of the onboarding process. We have also seen the growth of Open Banking in the UK, enabling new service offerings that allow users to securely share their bank-verified Digital ID details in any online user journey. Digital ID solutions have played an incredibly important role during this pandemic and are now seen as tested, proven and effective on the world stage.

Two years on from techUK's last White Paper it is clear that the benefits of Digital ID technologies, the resultant opportunities to the UK and its role in supporting and enabling the ongoing development of the UK's digital economy as well as its societal and innovation agenda have also continued to increase markedly as a result.

The Global Digital Identity Market is estimated to be worth USD 16.6 billion in 2021 and is expected to reach USD 40.44 billion by 2027, growing at a CAGR of 16%.[6] However, whilst the economic and social benefits of Digital ID continue to evolve, the UK is still facing challenges that existed before the pandemic which have not gone away, especially the impact and cost of online fraud.

Online fraud has a profoundly corrosive effect on the public's trust and subsequent willingness to engage with digital innovation. We should be in no doubt that if we do not find an effective solution to significantly reduce the instances of online fraud that cause both harm and hardship to many of our friends, family, business associates and their respective employers then Government and Industry risk losing the public's trust even further and experiencing substantive damage to the financial and social fabric of our innovative, entrepreneurial, and forward-looking society.

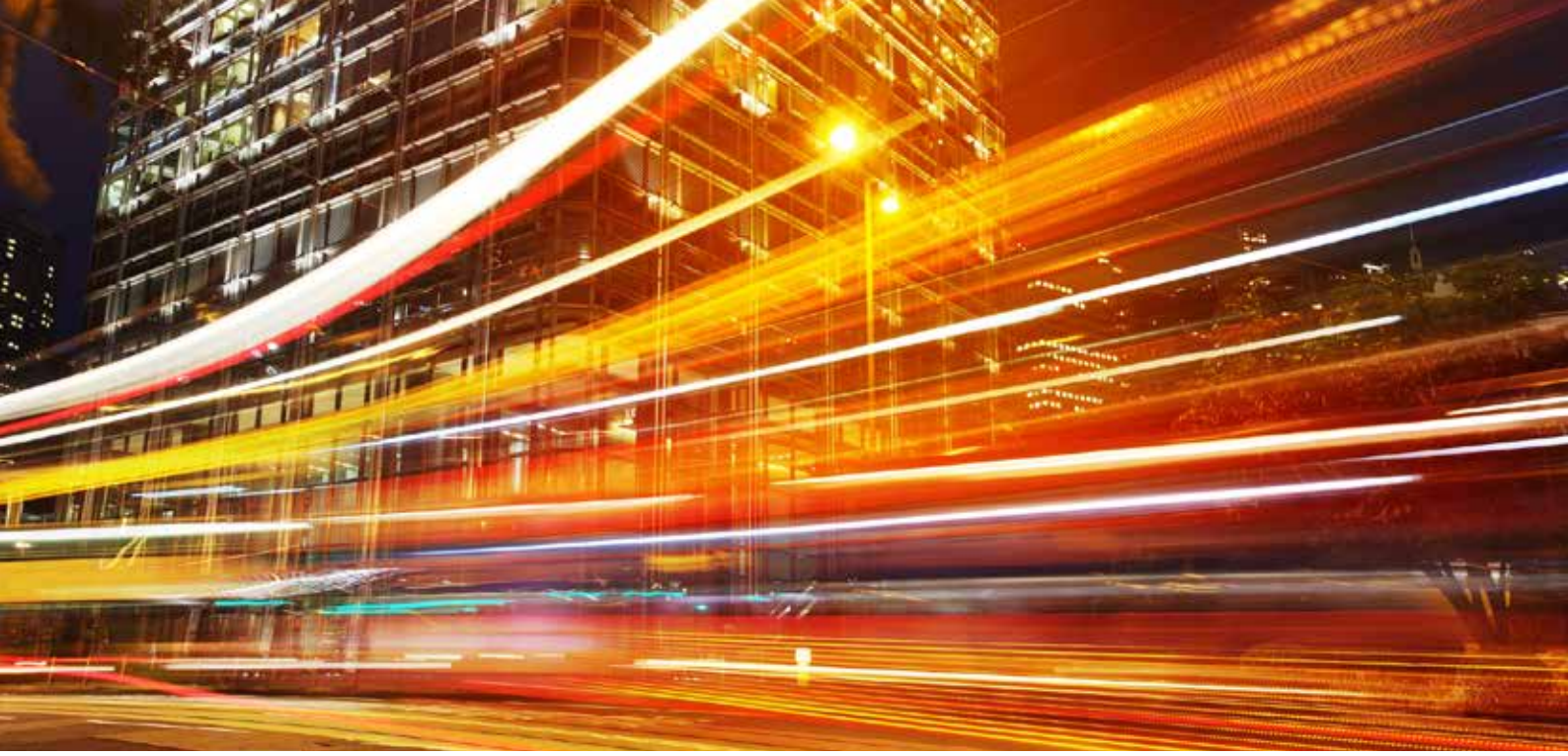
However, the good news is that innovation in Digital ID has become a powerful tool in the war against fraud, even in an as-yet unregulated marketplace. Whilst the creation of a secure regulated Digital ID market in the UK won't irrevocably extinguish the ability of criminal enterprises to defraud businesses and citizens entirely, the effective implementation of an optimised regulatory and legislative governance, coupled with the technical and go-to-market innovation inherent the UK's Digital ID Industry can provide a robust and effective line of defence against the scourge of online fraud and reduce its impact significantly.

Whilst Government and industry have made good progress in this so far, we are not at the finish line yet and it is vital that we maintain our focus to see the job through to a successful conclusion, namely the creation of a robust, effective and flexible regulatory framework in the UK.

Should the UK fail to get Digital ID right at this stage in its development and miss the opportunity to drive forward the Digital ID market in the UK – and by extension the robust, trusted and user-friendly digital economy that it will enable – there is a very real risk that the UK falls even further behind those competitor jurisdictions around the world who have not been slow to appreciate the fundamental importance of Digital ID to their economies.

Despite the high stakes there is room for optimism however, particularly given the progress made since our first Digital ID report back in 2019.

In the past two years, we have seen DCMS adopt a more open engagement strategy toward the Digital ID Industry in the UK, and we encourage all Government departments to adopt and expand on this approach. We have seen the publication and continuing development of the UK Government's UK Digital ID & Attributes Trust Framework (currently in Alpha 2 iteration). We also saw in December 2021 the announcement that the Trust Framework would be used to support the Home Office Right to Work and Right to Rent schemes and DBS (criminal record checking) pre-employment checking[7] from 6th April 2022.



Additionally, the Government's announcement on the 10th March 2022 of the publication of its formal response to Digital ID and Attributes Consultation (July 2021) included its intention to introduce legislation to create a legal gateway allowing certified ISP (Identity Service Provider) access to data attributes and/or verification held by government departments, for that data to hold legal equivalence to existing physical documentation and the use of a Trustmark for ISP's certified under the Framework, all of which were called for in previous techUK white papers and our formal Response to the 2021 Consultation. Whilst the government has indicated its preference for a governing body that owns and administrates the Trust Framework within an existing regulatory body – something that techUK and other key stakeholders believe would be better served by separate regulatory and governing bodies - it has decided to create a new interim governing body within DCMS in the form of the Office for Digital Identity and Attributes (OfDIA).[8]

Progress has also been made with individual Government departments own identity schemes and the development of the GDS's One Login for Government scheme, we will examine this further in the next chapter. In parallel, we are witnessing the ongoing development of a burgeoning Digital ID ecosystem in the UK, with a proliferation of Private Sector Digital ID solutions being deployed by forward-thinking organisations who recognise its fundamental importance to their business.

However, now is not the time for complacency. Far from it.

We must continue to move forward at pace given the opportunity that Digital ID represents to the UK economically and socially. Whilst action has been taken and progress made, there is still work to be done if we are to position the UK for success in Digital ID for Industry, Government and Citizens.

To determine what action is needed to ensure this happens this report will:

- Review today's UK Digital ID Ecosystem and identify remaining challenges
- Assess progress made since techUK's 2019 and 2020 White Papers
- Propose clear calls to action so that workable, real-world solutions to these challenges can be found, enabling a UK Digital ID market that can thrive long term in the UK and upon which a vibrant and inclusive digital economy can flourish

The UK's Digital ID Ecosystem in 2022

Before considering the progress made in respect to the recommendations made in techUK's 2020 White Paper, and therefore what action still needs to be taken and by whom, it is important for us to reflect on how far we have come in the past three years. We will examine what the UK's Digital ID Industry and ecosystem looks like today, the real-world positive examples of Digital ID in action that we have witnessed, particularly during the pandemic, and the positive impact that Digital ID solutions are realising for both businesses and individuals right now.

The following is a snapshot of the UK's Digital ID ecosystem and market today, including some latest examples of developments in Digital ID in action across both the Public and Private Sector. The aim of the following is to demonstrate the activity and action that has taken place across the UK in the last two years.

Digital ID in the UK Public Sector

Since 2020 there have been two key areas where progress has been made in the deployment of Digital ID by the UK Government and the wider Public Sector. These are:

- Government as Enabler of Digital ID market
- Government as Consumer of Digital IDs

Government as Enabler of Digital ID market

Policy Developments

In 2021 the Department of Digital, Culture, Media and Sport (DCMS) announced the publication of an Alpha Digital ID Trust & Attribute Framework. techUK members and other industry stakeholders were invited to review and propose necessary amendments to and enhancements of the Framework and saw its publication as an important step forward in the UK being able to realise the full potential of Digital ID.

The Framework is now expected to move to a Beta version during the Spring of 2022 and techUK welcomes the sustained efforts of DCMS to work with the UK's Digital ID Industry in the development of the Framework to date.

In addition, the recent publication of DCMS' formal response to the Digital Identity & Attributes Consultation makes clear the Government's intention to advance/amend legislation to support the development of private sector access to Government data attributes for identity verification, the creation of an interim governing body within DCMS – the Office of Digital Identity & Attributes (OfDIA) – to oversee further development of the Framework, legal equivalence for digital identity credentials with physical documentation and more.

This is a definite step in the right direction, but without a clear plan and timetable of implementation it remains an intent only, albeit a publicly stated one. What UK Citizens and industry need right now is certainty and positive action around Digital ID, mere intent is simply not enough.

Government as Consumer of Digital IDs

Public Sector adoption of Digital ID

Across the UK Public Sector there has been marked progress in the number of new Digital ID schemes developed and deployed by various Government departments. These include:

- NHS Login – now with circa 28 million registered users[9]
- Home Office – Digital IDs for Right to Work/Right to Rent/DBS Checks[10]
- HM Land Registry – Digital IDs for Conveyancing[11]
- EU Settlement Scheme - EU Exit App[12]
- Home Office – Generic Identity Verification Service (GIDV)[13]
- Home Office – Sandbox for Retail Age Verification[14]
- Pensions Dashboards Programme[15]

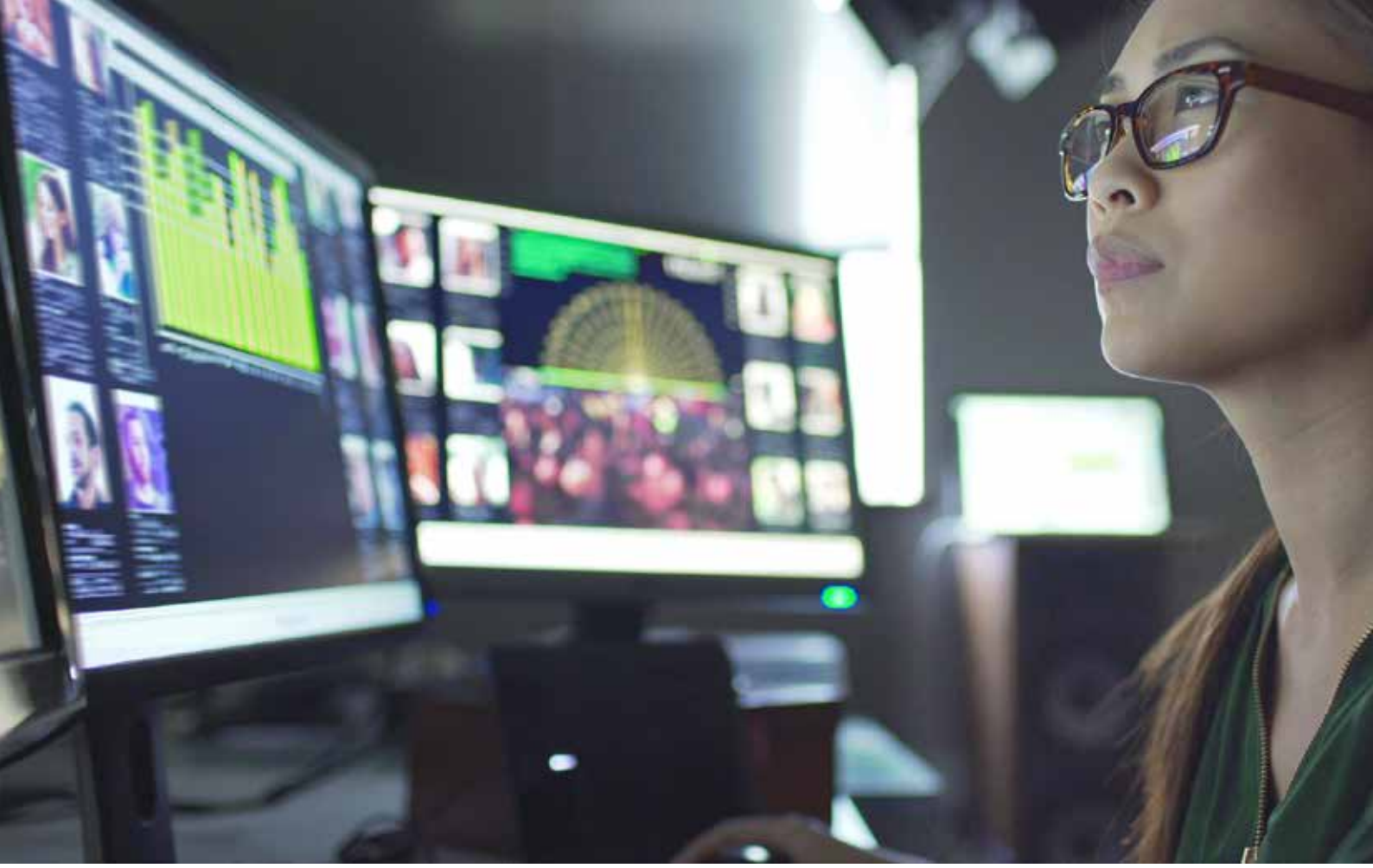
The use of Digital ID technology in support of the NHS Login service, particularly during the COVID-19 pandemic, provides us with a strong use case to demonstrate the profound impact that Digital ID solutions can have on people's lives. That 28 million users have now registered for this service demonstrates a significant pent-up demand for safe, secure, and easy-to-onboard public services utilising Digital IDs for identity verification.

This use case shows that if Citizens see real value in engaging with a Digital ID solution and if the service is supplied and/or governed by an entity that the public feel that they can trust then adoption of a Digital ID enabled service or solution can happen far more quickly and effectively than previously thought possible.

Another area where significant progress has been made is in the recent announcement by the Government to schedule and implement legislative changes to allow the Home Office to accept digital identities (Identification Document Validation Technology or IDVT), from Digital ID Providers (ISPs) in lieu of physical documentation for Right to Work, Right to Rent and DBS (i.e., criminal record) checks from 6th April 2022. This is a significant move forward and has been welcomed by Industry.

However, there remain several questions about how this scheme will function and what this means for Industry and market competition. For example, it is understood that additional changes to primary legislation will be needed to mandate the use of Certified ISP's by relying parties, if relying parties so choose to use digital identities, meaning that further clarification here is essential.

The announcement made by DCMS on 10 March 2022 of the Government's intention to bring forward legislation to establish a "robust and secure accreditation and certification process and trustmark" to ensure this to happen is welcomed. However, further detail is still needed.[16]



Another serious concern centres on the Government not accepting Digital IDs supplied by ISPs certified under the UK Trust Framework being developed by DCMS. If this is not addressed this could significantly restrict market growth. This approach also suggests a less than coherent approach to interoperability and the Governments own stated intention to allow Digital IDs to be transferable.

> **This is an area where the Digital ID Industry and market need clarity and certainty on the timelines and processes involved so that businesses and their customers can confidently plan ahead and invest accordingly.**

Gov.UK Verify to One Login for Government

In addition to the number of individual Government departments initiatives, since 2020 change has been observed in relation to the UK Government's Gov.UK Verify scheme.

In 2018 the Government announced that it would cease funding for Gov.UK Verify during 2020, but due to the pandemic this deadline was extended to April 2022.

In February 2021, then Minister for the Cabinet Office, Michael Gove stated that all public-facing central Government services would have to migrate onto the new Digital ID platform, subsequently announced as One Login for Government.[17]

In March 2021, Cabinet Office Parliamentary Secretary, Julia Lopez, confirmed that Gov.UK Verify would be scrapped and replaced with a new Government Digital ID platform to be used across all Government departments. Previously publicly reported costs for the Gov.UK Verify build were put at £220m+.[18]

The One Login for Government platform is in ongoing development as an internal project build within GDS except for a recent tender[19] to produce a smartphone app for One Login for Government from which UK Citizens can access all Government department services from passports in a similar manner to that utilised in the Home Office's EU Exit app during Brexit. Whilst two further tenders have been awarded during April 2022[20] - another to Deloitte and one to consultancy 6 Point 6 – neither of these were awards to companies whose core business is Digital ID.

Recent announcements from GDS regarding their One Login for Government service development appear to go some way to addressing the issue that almost every Government department is developing its own Digital ID scheme for those Citizens who access their services online under the GOV.UK banner. However, it is as yet unclear as to whether those same Government departments will be obligated to adopt One Login for Government so, as we saw with GOV.UK Verify, should they choose not to do so and continue to use their own proprietary solution instead this could risk seriously undermining the credibility of the new platform in the eyes of the public as, by definition it would have failed to provide the single sign-on experience originally envisioned and articulated by GDS.[21] As discussed later in this report this is a significant issue and area of concern for techUK where greater clarity and further action may still be required.

Of all the activities happening across the UK Government involving Digital ID today, the development of the GDS' One Login for Government platform is an area where industry has struggled to navigate, engage with and understand how it will work in practice from a technical perspective and interoperate with other Digital ID schemes across both Public and Private sectors.With recent reports quoting a budget of circa £400m[22] for GDS to build the platform internally and, as yet, no official indication that Private Sector platform providers will be asked to tender for the One Login for Government platform build, (other than for the tender awards mentioned previously), there is significant confusion and concern about why GDS would not seek to utilise the skills and expertise of the UK Private Sector to build such a significant technological undertaking. To take this approach at a time when the Chancellor of the Exchequer is seeking to extract maximum taxpayer value from Government services and where existing Private Sector solutions could be utilised at a fraction of the projected cost to keep it an internal build appears antithetical.

The approach being taken by UK Government on the development of One Login is very different from that seen in other markets. For example, the EU is encouraging Digital ID trials and pilots via a public/private partnership approach throughout the 27 Member States and is offering grants to match 50% of the costs.[23] This is an excellent example of a partnership approach that is supported by industry and one that we would encourage the UK Government to recognise and adopt as a matter of urgency to support market development.

Private Sector Digital ID Market and Industry

Since 2020 the Private Sector Digital ID ecosystem and sector has continued to grow, scale and innovate. Digital ID technology and solution providers have delivered significant benefits to UK businesses and customers who require more robust and user-friendly Digital ID solutions at scale, particularly as the scale of online fraud continues to grow.

Development and innovation has been seen particularly in biometrics, facial and voice in recent years. This has enabled the development of a new generation of Digital ID solutions that promise significantly greater protection from online and physical fraud and other forms of identity misuse. It should be noted however, that the lack of a modern regulatory framework capable of creating a viable and secure biometrics ecosystem is a barrier to delivery of the very real benefits that biometrics can bring our society.

Whilst adoption, deployment and take-up of Digital ID solutions is happening today across various UK sector verticals, uptake in the Financial Services sector has been much slower than anticipated.

Many in the sector posit that anxiety around adoption is very likely due to the regulatory requirements to conduct thorough Anti-Money Laundering (AML) and Know Your Customer (KYC) checks on new customers as many firms have so far proved reluctant to hand over these critical processes to third parties, historically favouring white labelled services in preference to interoperable digital identity wallets. However, the industry body Joint Money Laundering Steering Group (JMLSG) have recognised in their 2020 revised guidance[24] that the use of digital identity and robust biometric technologies provided useful additional data attributes to assist firms in the Financial Services sector when considering using such processes. It is hoped that this will help drive greater adoption of Digital ID in the Financial Services sector.

techUK 2019 & 2020 White Papers – What Progress Has Been Made?

Given the current state of play of the Digital ID market across both Public and Private Sectors, progress has clearly been made in the adoption and usage of Digital ID by UK Citizens.

But much greater action is still required.

The Digital ID market is estimated to be worth around £60 billion to the wider economy with an attendant estimated GDP bump of between 3% by 2030.[25] For it to thrive, the right legislative, regulatory and market enabling ecosystem must be created. In addition, all barriers to the creation of a thriving Digital ID market must be identified and removed.

Before considering the action that is now urgently needed to enable and support the development of a long-term Digital ID market and Industry in the UK, it is important to assess the progress that has been made with respect to the recommendations made in 2019 and 2020.

The following assessment evaluates where progress has already been made and highlights those areas where still more work remains to be done. It also identifies key issues and areas which have arisen since the publication of our 2020 report that must now also be addressed.

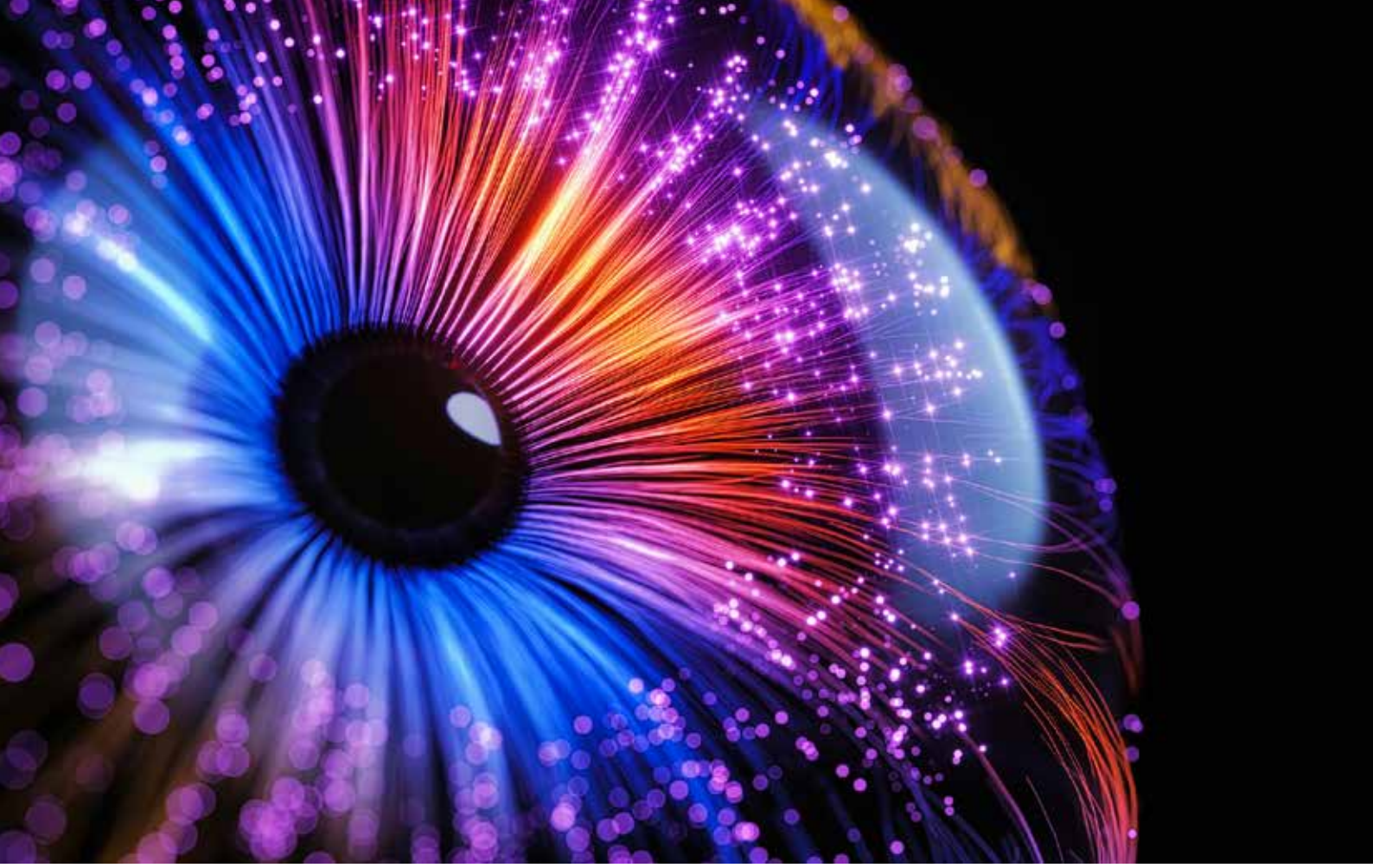
This report will then discuss and make recommendations on where action is urgently needed and identify which stakeholders need to take a lead to ensure real change is delivered in as short a timeframe as possible.

Topic	Year - Page	Recommendation	White Paper - 2020 Update (Latest)	2022 Status	2022 Comment
Access to Government Data Attributes	2019-4	Provide plans for the further opening 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 HMPO 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.		The Document Checking Service pilot continues to make slow progress, covers HMPO (Passport Office) only, and is simple yes/no response. DCMS Consultation Review Response (10th March 2022) announced creation of a 'Legal Gateway' to enable Certified ISPs to access Government Department data attributes/credentials. However, there is no clear plan or timeline indicated and uncertainty remains as to whether individual departments will make such data available as such provision will not be mandatory. It should be stated that this represents an 'intent only' thus far although DCMS' recent announcement that supportive legislation will be forthcoming during the 2022/23 parliamentary session will pave the way for the Legal Gateway but uncertainty remains over what Government data will be made available.
	2020-4	Accelerate work to allow private sector providers access to scalable interfaces into government databases (e.g., HMPO, DVLA).	As above		As above
Attributes	2019-5	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		Attribute provision is covered by the UK Digital Identity & Attributes Trust Framework but is one of the areas that needs greater clarity before it becomes usable
Central Government ID	2019-3	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).		There is significant concern that the engagement with industry by GDS on the building of the One Login project has been insufficient and lacking. Concern has also been expressed publicly that the mistakes of Gov.UK Verify are being repeated (at significant cost to taxpayer) with the proposed One Login for Government platform build intended to be built in-house by GDS.

Topic	Year - Page	Recommendation	White Paper - 2020 Update (Latest)	2022 Status	2022 Comment
Communications	2019-9	Plans should be put in place for government-led communications to raise public awareness of the importance of digital identity.	No Government action		No plans as yet for Government-supported communications to introduce/explain digital identity topics and encourage citizen adoption.
Enabling non-Gov Dig ID use for Gov use cases	2020-2	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.	No Government action		There is no indication from Government that Digital IDs from a DCMS-certified ISP will be usable to access Government Department services online. This approach is antithetical to the one proposed by the Minster for Digital Infrastructure in the Ministerial Foreword of the UK Trust Framework when he stated, 'The Government Digital Service's One Login system for government will also align with and help inform trust framework rules as they develop.'
	2020-7	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.	No Government action		As above
	2020-8	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.	No Government action		As above

Topic	Year - Page	Recommendation	White Paper - 2020 Update (Latest)	2022 Status	2022 Comment
Governing Body	2019-2	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.		DCMS' Digital Identity & Attributes Consultation of 10th March 2022 announced its intention to create an interim governance function within DCMS, to be named the Office for Digital Identities and Attributes (OfDIA) to be supported by a public/ private Advisory Body. However, no detailed plan or timetable has been shared yet with industry
	2019-8	Nominate a competent independent authority for digital identity.	No Government action		As above
	2020-5	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.	As above		As above
International Interoperability	2020-6	Work in collaboration with international governments, non-government organisations (NGOs) and standards bodies to enable interoperability of digital identities internationally.	No Government action		DCMS are working with Singapore and other Governments on international interoperability via trade agreement discussions, little visibility on how industry can input to this process as yet
	2020-9	Ensure that the future Trust Framework is interoperable with the EU, by making it the UK's new notified scheme.	No Government action		No clarity on UK/International discussions.

Topic	Year - Page	Recommendation	White Paper - 2020 Update (Latest)	2022 Status	2022 Comment
Biometrics	2019-7	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		No Government action
Legal Equivalence	2019-6	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		DCMS' Digital Identity & Attributes Consultation (10th March 2022) states 'We will therefore require such private sector organisations to become certified against the trust framework before they are able to make checks against government-held data through the proposed legal gateway.' The legislation designed to allow the creation of the Legal Gateway is now timetabled during the 2022/23 parliamentary session.
	2020-3	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.	No Government action		DCMS Consultation Response stated, 'We will therefore seek to introduce legislation, when parliamentary time allows, to affirm that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents.' but following the 2022 Queens Speech DCMS have confirmed that supportive legislation is now timetabled for the 2022/23 parliamentary session.
Policy	2020-1	Put digital identity at the heart of the upcoming Digital Strategy and the Data Strategy.	No Government action		No Digital Strategy has so far been published. Digital ID mentioned briefly once in the National Data Strategy published on 9 December 2020.
Trust Framework	2019-1	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).		The UK Digital Identity & Attributes Trust Framework was originally published on 11th February 2021 with the Alpha 2 iteration published on 8th September 2021. DCMS have indicated that publication of the Beta iteration is expected in Spring 2022.



What we need now

Based on the assessment of progress made since 2019 and 2020, clearly some significant steps have been taken and progress has been seen, particularly in relation to engagement between Industry and Government, driven by the development of the UK Trust Framework.

Since 2020 the digital Industry has witnessed a consistently improved engagement strategy on the UK Trust Framework from Government, for which officials from DCMS should rightly be acknowledged.

This engagement has been helpful in terms of the development of the robust and flexible regulatory and legislative governance framework that will be needed to deliver the 'world-class' Digital ID ecosystem in the UK that Industry and the Government both want.

And whilst some of the calls to action techUK made in 2019 and 2020 have been both listened to and acted upon, it is the opinion of techUK that action is still urgently needed and needed now to address both outstanding and newly evolved issues that have arisen in the past two years particularly around the applicability – or otherwise – of sections of the Framework to those companies operating a B2B as opposed to B2C business model.

> **techUK believes that it is now imperative that the full implementation of the Trust Framework must happen during the first half of 2023.**

> **To ensure that this happens, DCMS will need the Ministerial backing and dedicated resources necessary to significantly reduce the timeframe for this implementation, of the legislative changes required to support it and the creation of a permanent independent governance body to help both Industry and Government navigate the technological, societal, regulatory, and legislative challenges that will undoubtedly impact the UK Digital ID ecosystem as it evolves.**

Accordingly, the ability to further optimise the Framework to allow for these changes must be built-in, with a governance structure that includes both public and private stakeholders able to react quickly and effectively to market change.

There are many real-world examples of Digital ID in action today across the UK that demonstrate the power of this technology. It is not hard to imagine what more could be done when the digital Industry is able to plan confidently and invest longer term in how Digital ID solutions can best be deployed across all sector verticals.

However, this will not happen unless action is taken in several areas where Industry still sees a lack of certainty as to the way forward, particularly in relation to the timeline associated with the legislative changes required to fully support the Trust Framework, but also with certified ISP's having their Digital IDs accepted by Public Sector identity schemes, including for One Login for Government.

The following chapter examines these remaining challenges and outlines techUK's proposed actions to address them.

Overcoming challenges - 2022 Recommendations

We made it clear in techUK's 2020 White Paper that substantive, co-ordinated action is required from both Industry and Government to ensure that the UK can fully realise all of the economic opportunities and social benefits that a properly regulated Digital ID market can deliver.

Despite the progress that has been made, it is the view of Industry that the pace of change is still too slow, and their plea now is for more sustained and co-ordinated action to deliver the minimal viable Trust Framework, as called for in techUK's response to DCMS' Digital Identity & Attributes Consultation, during the first half of 2023.

techUK has identified the following areas where we believe action must and can be taken to deliver this vision during 2023;

1. **DCMS to create a formalised timetable to enable the full implementation of the UK Digital ID and Attributes Trust Framework during the first half of 2023**
2. **As DCMS have recently indicated, the associated legislative changes required to support the UK Trust Framework should be timetabled during the 2022/23 parliamentary session**
3. **GDS's One Login for Government platform build should be fully opened to competition and tender process**
4. **Certified ISPs should be granted access to government department-owned data attributes/ credentials under the proposed 'Legal Gateway' during the first half of 2023**
5. **The creation of a permanent Public/Private Governing Body which owns, defines, promotes, and certifies against the Trust Framework during the first half of 2023**

6. Government to allow full interoperability between Public & Private Sector Digital IDs
7. A detailed plan and timetable to create a unique, independent UK Regulator to oversee UK Digital ID ecosystem by the end of 2023
8. Government proposals on the future of the UK Data Protection Act must provide more clarity to UK ISPs on areas that may impact the use of Digital ID in the UK
9. Public engagement to build public trust and confidence in Digital ID must be prioritised by Government Communications Service and a plan put in place for 2023
10. DCMS and industry stakeholders to create a formalised joint working group to co-operate and accelerate delivery of the UK Trust Framework during 2023

The following sections detail the context in which these recommendations are made.

1. DCMS to create a formalised timetable to enable the full implementation of the UK Digital ID and Attributes Trust Framework during 2023

The development of the DCMS Trust Framework with input from the Private Sector over the past three years has been welcomed by Industry and the impending development from the Alpha to Beta phase of this process will be another important step forward. However, it is important that as the Framework moves to the Beta stage that all outstanding issues and concerns raised by industry with the Alpha version are resolved and a clear and binding implementation plan and timetable be created and, importantly, shared with Industry.

Whilst Industry has welcomed the consultative approach that DCMS has taken to the development of the Framework to date, Industry is looking for certainty and clarity that the Framework will be completed and implemented fully during 2023.

Industry would like to see DCMS take an approach where a minimum viable route towards launch of the Framework can be found. It is important therefore that this approach ensures that all necessary standards are in place and are ideally globally recognised (rather than just UK specific) to promote scalability beyond the UK.

Furthermore, Industry would like to have greater clarity and transparency on international standards for digital identity and to be able participate in its development as with the UK Trust Framework.

Any timetable being developed should cover not only the full implementation of the Framework itself, but also any remaining legislative and/or regulatory changes that will be required to enable Government departments to accept Digital ID's in lieu of physical documentation and amend their internal business processes accordingly. This should also include provision for regular reviews of the Framework, preferably annual.

To ensure that the Framework moves forward efficiently and the progress sought by industry can be achieved, it is vital that the Digital ID team within DCMS are resourced effectively to ensure the Trust Framework successfully moves from its Alpha to Beta stage. Given the importance of speed of legislation in the process of the Framework's full implementation, it is vital that DCMS are given the resources and support by civil servants that will be needed in this new phase.

Recommendations

A clear and detailed formal timetable for the rest of 2022 is needed from DCMS on the steps that will be taken to ensure that the Framework can be finalised and implemented during the first half of 2023.

techUK believes it is imperative that DCMS receive the required support, both financial and political, from Government at the highest level and calls on the Secretary of State for DCMS to make this a key priority for Government.

2. The associated legislative changes required to support the UK Trust Framework should be timetabled during the 2022/23 parliamentary session

We are presented then with an unprecedented opportunity to lead the world in the development of our digital economy. But for this to happen we must create the optimal regulatory and legislative landscape to fully enable the UK Digital ID Industry to deliver its world-class solutions to UK Citizens and businesses.

It is now clear that the legislative changes required to support the UK Trust Framework must be made to legislation. The announcement by DCMS on the 10 March to introduce legislation is welcomed as is their confirmation following the 2022 Queen's Speech that supportive legislation for digital identity will be forthcoming during the 2022/23 parliamentary session as part of a data reform bill.

Recommendation

The pace at which regulatory and legislative changes are to be implemented must increase. This requires greater political will at the highest level of Government to drive a co-ordinated and coherent overall Digital ID strategy across all areas of Government that is fully aligned with both existing and developing Data policy that impacts the implementation and adoption of Digital ID in the UK.

3. GDS's One Login for Government platform build should be opened to competition and tender process

To date, there has been minimal Industry engagement by GDS regarding the technical development of the One Login for Government project and there remains considerable concern at the lack of transparency and openness as to the technical specifications of the project. For example, no details have been provided on the technological requirements of the project and little information shared with Industry on how they can help to provide the One Login for Government project.

techUK believe that GDS should utilise existing Private Sector Digital ID solutions and platforms that already exist in the market instead of either creating a new solution from the ground up or – in our view a far worse outcome – build a GDS solution internally that builds on the soon-to-be phased-out Gov.UK Verify platform.

Private Sector Digital ID platform and service providers possess the technical, commercial and implementation skills and experience that could support the development, building and delivery of the optimal iteration of the One Login for Government platform.

Many Digital ID technology providers have already supplied either platforms and/or important technology elements to Government department Digital ID schemes. To not be able to tender in the same way for the One Login for Government platform initiative appears both antithetical and in opposition to the spirit of Public/Private partnership seen elsewhere across other Government technology developments.

With the Chancellor of the Exchequer recently announcing a new drive on efficiency, effectiveness and economy in Government spending from the new Efficiency & Value for Money Committee that he chairs[26], the £220m already spent on the soon-to-be-defunct Gov.UK Verify coupled with the widely reported[27] budget of up to £400m for the GDS build of the One Login for Government platform doesn't appear to represent good value for UK taxpayers.

To date there has been a lack of openness by GDS as regards to the technical specifications and overall approach being taken to the project going forward techUK calls on the GDS to open up the platform provision element of this project to an open tender process.

Recommendation

GDS should use existing Private Sector Digital ID solutions for One-Login and open up the platform provision element of this project to an open tender process.

4. Certified ISPs should be granted access to government department-owned data attributes/credentials under the proposed 'Legal Gateway' during the first half of 2023

In our 2020 White paper, techUK called for acceleration of the process '… to allow private sector providers access to scalable interfaces into government databases (e.g., HMPO, DVLA)' as an important additional identity verification source, reiterating this call again in our additional Consultation Response in September 2021.

Whilst the recent DCMS Consultation Response stated their intention to develop a 'legal gateway' to allow Private Sector certified ISPs to access Government departments data for identity verification purposes, no clear plan or timetable has yet been communicated to Industry and this development will also require legislative amendments though DCMS has recently stated that these will be timetabled during the 2022/23 parliamentary session.

It is the view of techUK that UK Government credentials/attributes be made available to certified Digital ID Providers at the earliest possible opportunity.

This applies especially to both UK Passports and Driving Licences. The early introduction of digitised versions of these two, both historically trusted and familiar physical credentials long trusted by UK Citizens, will go a long way to helping Citizens to understand and develop trust in using Digital IDs going forward.

Recommendation

Certified ISP's to be granted access to Government identity attribute data at earliest possible opportunity.

5. The creation of a permanent Public/Private Governing Body which owns, defines, promotes, and certifies against the Trust Framework during the first half of 2023

techUK have consistently called for the creation of a Public/Private partnership body to own and administrate the Trust Framework – see both our 2020 White Paper and our Consultation Response from September 2021 – allowing the, yet to be appointed, regulator to enforce the Trust Framework.

The announcement made by DCMS on the 10th of March 2022 on the setting up of an "interim government body for digital identities", the new Office for Digital Identity and Attributes (OfDIA) is a welcome development. However, as DCMS clearly state that this is an interim body only, more visibility on how and when the permanent body will be implemented is required by Industry.

It is vital that a permanent governing body is developed and put in place, and that this should be a priority as outlined in techUK's Consultation Response last September 2021 which called for a governing body to be constructed '…as a public/private partnership between HMG, the identity industry, relying party representatives and consumer representatives. Scheme leads should also be represented as part of this partnership.'

The creation of an effective independent governance structure will be key to building public trust and confidence in this emerging Industry long term. The creation of a permanent, public/private partnership governing body is therefore required as soon as is practicable.

Recommendation

Industry and DCMS must engage as a matter of urgency to draw up plans for the creation of a permanent Trust Framework Governing Body with representatives from Government, the Digital ID Industry, Relying Party and Consumer Representatives in time for the full implementation of the Trust Framework by the end of 2023.

6. Government to allow full interoperability between Public & Private Sector Digital IDs

In DCMS' recent Consultation Response, the following high-level objective was highlighted – 'Enable interoperability to ensure optimal outcomes from the perspective of the end-user/data subject'.[28]

techUK is supportive of this objective. However, techUK Members cannot therefore understand why Government have chosen not to allow Private Sector Digital IDs to be used to access Government services and vice versa. This does not represent true interoperability and can only create confusion and doubt in the eyes of UK Citizens who are looking to the Government for clarity around Digital IDs.

If the UK Trust Framework, created by DCMS with input from a wide range of Industry stakeholders and overseen by the new Office for Digital Identities & Attributes (OfDIA), can certify Private Sector ISPs and demand as an integral part of that certification process, strict adherence to 'the highest standards of security and privacy' and issue an easily recognisable Trustmark so that UK Citizens can trust their services, then techUK believes that these services/attributes/identities from Government-certified service providers should also be acceptable for other Government Identity Schemes, including the proposed One Login for Government.

Recommendation

Government should allow Private Sector Digital IDs to access Government services and vice-versa, and amend any remaining legislative barriers accordingly

7. A detailed plan and timetable to create a unique, independent UK Regulator to oversee UK Digital ID ecosystem by the end of 2023

In addition to the creation of a governing body as outlined above, it is important that a unique, independent regulatory body is formed by Government to enforce the Trust Framework as an entity separate from the governing body. Whilst the governing body for digital identity should own the trust framework itself, a regulator is needed to set out the principles and legislation under which the governing body must operate and evolve the trust framework.

In our 2021 Consultation Response, techUK made a clear call for a two-step approach to the formation of a UK Regulator for Digital ID. As an interim step, in the short term, we recommended that a distinct unit should be formed within the Information Commissioners Office (ICO) to work with the Trust Framework Governing Body to oversee and enforce as required.

However, in the longer term, there should be a full Industry and stakeholder consultation process enacted to determine the need for a new, separate regulator for Digital ID in the UK by the end of 2023. In order to ensure this happens techUK would like to see the creation of a dedicated working group between Government and industry to consider the right long-term approach on this key issue.

Recommendation

DCMS to engage with Industry to form a working group with key stakeholders to develop plans for submittal to Government based on the recommendations above.

8. UK Government proposals on the future of the UK Data Protection legal framework must provide certainty to UK Digital ID providers on the impact of possible changes

In September 2021 DCMS published for consultation the report "Data: A New Direction" which explored possible changes to the UK's data protection legal framework. Whilst techUK welcomed the conversation that the consultation launched, the issues it raises around the data protection requirements that Digital ID providers may be required to follow in the future has raised some uncertainty. For example, there is some concern that possible changes may make it difficult for the Digital ID Industry to assess its impact on the Private Sector provision of Digital ID services. This has the potential to slow the growth of the market and ISP's willingness to invest due to the regulatory and legislative uncertainty, having only relatively recently absorbed GDPR regulation into their product processes and safeguards.

There is a pressing need for clarity on the new steps that may be taken with this work by DCMS and how any possible changes that may be proposed might impact the requirements within the current Trust Framework and the Digital ID Industry as a whole. It is important that any changes that are proposed to be made to the UK's Data Protection legal framework are reflected in the Trust Framework if that becomes necessary.

In particular, techUK urges DCMS to resolve continuing concerns with the Section 16:13 of the Alpha Trust Framework focusing on Privacy and Data Protection Rules as outlined below;

GDPR and the Alpha Trust Framework

There is continued concern that the approach being taken in section 16.13 is not aligned with the UK's data protection legal framework (UK GDPR and DPA18) and must be addressed and remedied as a matter of urgency. In particular, the sections on "Getting your users' agreements" and "Prohibited processing of personal data" do not recognise or reflect the different legal bases (such as legitimate interest or where processing is necessary for the performance of a contract) for the lawful processing of data that exist under the GDPR and current UK data protection law and should be amended. For example, what might be considered a 'user agreement' is unclear and is not a recognised term in data protection. Also, the focus on "user agreements", if this is to mean consent, only could limit the ability of organisations to protect individuals and should be reviewed.

The Trust Framework must be amended to align itself with current data protection law and provide legal clarity that an Identity Provider or Attribute Provider does not need to obtain consent from an individual where they are processing data under one of the lawful bases (such as legitimate interest) provided under the UK GDPR/DPA18 or where the relying party has already obtained consent typically through contractual or other GDPR legal bases. Also, the Trust Framework should be amended to provide clarity that relying parties do not need to obtain consent each time an individual's data is processed as this is not aligned with the UK data protection laws around consent. The way the Trust Framework is currently worded does not reflect the legal basis that already exist for how consent should be currently obtained and managed.In addition, there is concern with the statement on "Getting users agreement" that currently states that "you must get customers to provide positive confirmation that they have understood how their personal data will be stored and in what condition their digital identities or attributes will be shared or disclosed". While this may be possible for those B2C organisations that are user facing and/or manage user-controlled accounts, for other B2B organisations that do not have a direct user relationship obtaining such confirmation will not be possible. As a result, B2B organisations would be excluded from the Trust Framework. This is an issue that must be addressed to ensure that the Framework is appropriate and works for both B2C and B2B organisations.

Also amending section 16.13 so that it is not focused solely on the important role of "user agreements" but in addition recognises the other lawful basis for processing data under the GDPR that organisations can also help to increase users' data protection. Making it clear that organisations are able to also take different approaches (under the legal bases provided by the GDPR) to protect individuals' data, and not just focus on user agreements, would be welcomed. Currently the Trust Framework does not reflect the other way in which organisations can protect individuals from threats such as processing data for preventing fraud which is allowed under the GDPR. Redrafting section 16.13 to recognise all the legal basis that exist alongside the role user agreements can play would address this issue.

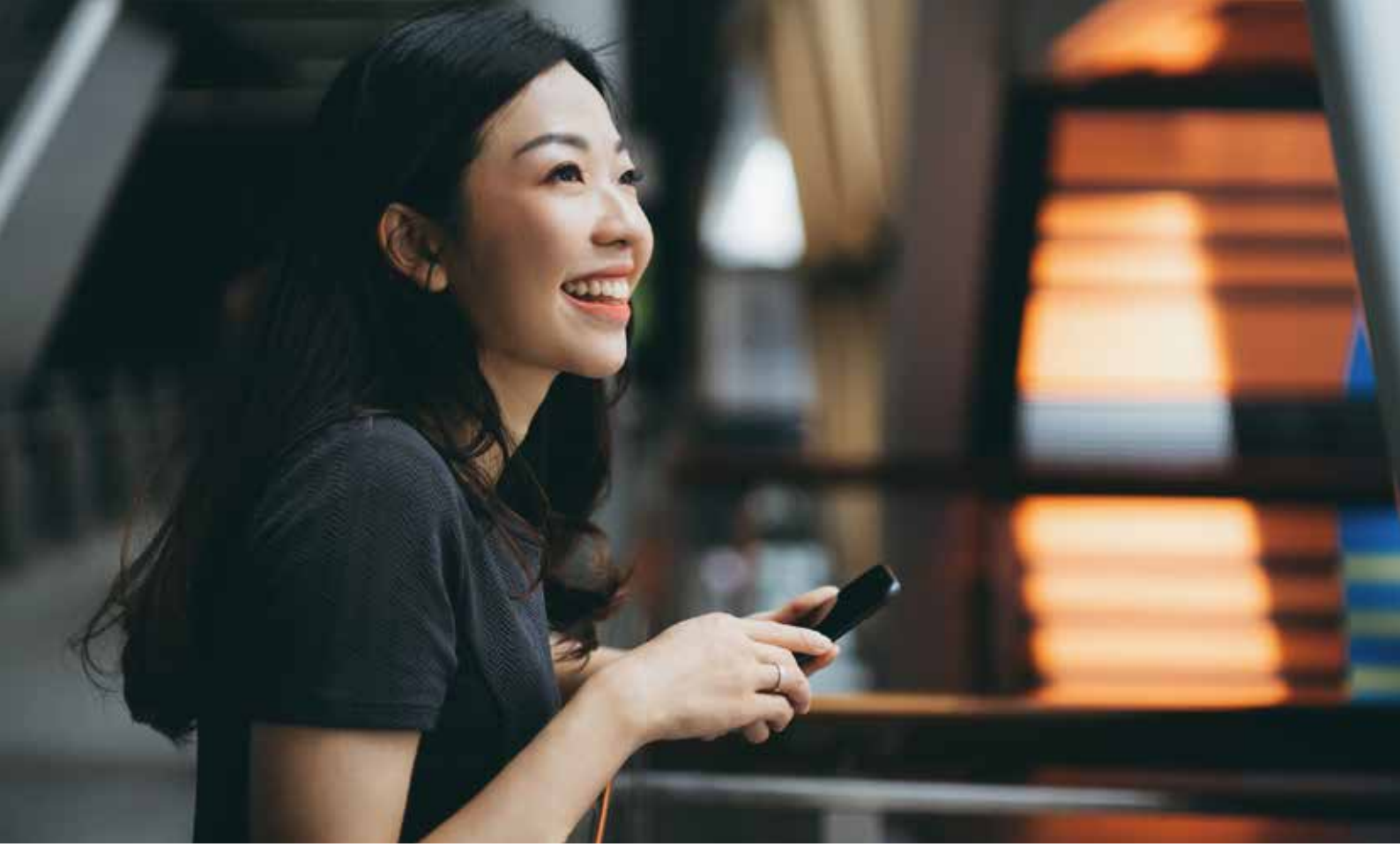
This issue has been raised by techUK with DCMS as recently as December 2021 and has not as yet been resolved. However, this is a key outstanding issue with the Trust Framework that must be resolved. To ensure users' data and privacy rights are fully protected the Trust Framework should align itself with the current UK Data Protection law. Section 16.13 of the Trust Framework should

therefore be amended to ensure that it does not unintentionally introduce additional, or possibly conflicting data protection requirements which could lead to legal confusion, uncertainty and unnecessary compliance burdens for organisations and as a result reduce the data protection of individuals.

Whilst our most recent engagement has been more encouraging, it is vital that DCMS include this change in the upcoming Beta version of the UK Trust Framework as the current wording clearly states that ISPs, ASPs and OSPs must hold a user agreement to process any personal data about an end-user. This wording must be changed to recognise that those companies certified under the Framework and operating a B2B rather than B2C business model should not be required to obtain end-user agreements as it simply does not reflect how, for example, how KYC and anti-fraud checks are dealt with today and that the applicable existing regulatory precedent set in DPA 2018 and UK GDPR should be used in these cases.

In its current form, many UK Digital ID service providers would be effectively barred from the market as they would be unable to achieve Framework certification and failure to amend this glaring oversight in the upcoming Beta version would be a huge blow to the credibility of the UK Trust Framework itself and immensely damaging to the development of Digital ID in the UK for which an effective regulatory ecosystem is crucial.Recommendation

- The upcoming BETA version of the UK Trust Framework should be amended to limit the requirement for User Agreement to be applicable only to those Relying Parties, ISPs, ASPs and/or OSPs operating a B2C model whilst using existing DPA 2018 and UK GDPR regulatory precedent to apply to those operating a B2B business model.
- DCMS to provide clarity on how any proposed changes to the UK GDPR and Data Protection legal framework might negatively impact the provision of Digital ID services in the UK. It is vital that any changes that are proposed to be made to the UK's Data Protection legal framework are reflected by DCMS in the UK Trust Framework at the earliest possible opportunity.



9. Public engagement to build public trust and confidence in Digital ID must be prioritised

The full economic and social benefits of Digital ID will only be realised if we bring Citizens with Industry and Government on this journey. The current public debate and discussion around Digital ID may have led to confusion and concern about what Digital ID technologies are and are not. It is important that we find ways to continue to shape the current public debate communicate and explain to the public the benefits of Digital ID technologies if we are to ensure take up and use of the solutions provided by a market enabled by the Trust Framework.

As we stated in our September 2021 DCMS consultation response it is the view of techUK that promoting the benefits of digital identity must be done at framework level, not scheme level. The governance body must do this as part of the Trustmark branding. Citizens are the key adopters of digital identity. Public communications must explain digital identity to an end user in a way that gives them confidence. The Government Communication Service (GCS) certainly has a role to play here, and we'd suggest the need for digital identity to be aligned to their government communication plans.

As stated elsewhere in this paper, we must remember that the true cost of fraud is not just the financial one but includes the potential for the serious erosion of public trust in Governments and Industry's ability to keep Citizens safe and secure online.

Restoring public trust in online will require concerted and co-ordinated action from all sides.

Citizens continue to use online services because of the efficiencies and convenience it provides, but they are wary and mistrustful of how their data is used – and misused – by the organisations with whom they transact and/or engage.

techUK believes that action from both Government and Industry to develop a strategy and tactical plan to help engage the public and build confidence in Digital ID as a tool that can help people in their everyday lives and protect people from serious threats such as fraud.

Recommendation

Industry and Government to develop a strategic communications plan - with key measurable outcome metrics, for public outreach and engagement by the Government Communication Service on the benefits and opportunities presented by Digital ID. Understanding public concerns and developing a strategy to build greater trust and confidence in the use of Digital ID will be key to ensuring long term adoption and use.

10. **DCMS and industry stakeholders to create a formalised joint working group to co-operate and accelerate delivery of the UK Trust Framework during 2023.**

techUK believes strongly that much time and effort in developing the UK Trust Framework could be saved by both DCMS and industry working together more closely to iron out remaining issues. It is imperative that DCMS understand exactly how the Digital ID ecosystem works so that issues and misunderstandings such as those seen with the recent User Agreement issue (see recommendation # 8 above) are identified and remedied quickly and efficiently.

Recommendation

DCMS and industry to meet at the earliest opportunity to agree how industry stakeholders can more efficiently input into the Framework development process directly under the auspices of a formalised joint working group.

Conclusion

As stated at the beginning of this report, techUK believe that the cornerstone of a future thriving, ethical and trusted digital economy in the UK, one where the principles of inclusion, privacy, security and interoperability are built-in and by-design, is absolutely predicated and reliant upon the ability of its Citizens, businesses and Government to be able to assert their identity online safely, securely and with an optimised user experience.

To ensure that this happens, the recommendations made in this report must be actioned by Government and supported by Industry to create the minimal, viable Digital ID ecosystem required in the UK today.

The costs of failure in this endeavour are, without exaggeration, dire indeed.

- Economic growth will be compromised, and the UK will fall even further behind the EU and other jurisdictions globally who are further advanced in their implementation of Digital ID
- Public confidence in transacting and engaging online will be further compromised as levels of financial fraud, identity impersonation and data breaches increase
- A fragmented and siloed Digital ID sector, lacking proper regulatory and legislative oversight, will continue to develop, but in an uncoordinated and fragmented manner, increasing complexity, costs and Citizen confusion

We have today, the opportunity to drive the pace of change within the UK Digital ID ecosystem and to make reality the worthy intentions outlined in DCMS' recently published Digital Identity & Attributes Consultation Response. But this will require concerted effort and focus from Ministers in Government to ensure that this technological foundation stone of the digital economy is as robust yet flexible, safe to use, secure and as inclusive as we can make it and that the proper regulatory and legislative oversight is in place to make this a reality.

As highlighted in previous sections, the ongoing uncertainty around the applicability of Framework section 16:13 to those operating a B2B business model must be resolved in the upcoming Beta version following significant industry representation to DCMS on this matter.

It is also crucial that the issues surrounding the full interoperability of the UK Digital ID ecosystem and the opening up of the One Login for Government platform build to open tender are addressed as a matter of urgency. Current Government strategy on these two points could discourage competition and innovation in the Digital ID market, create additional market complexity and confusion and may result in an unnecessary overspend of taxpayer money. The culmination of these factors risks further damage to Citizen confidence in Digital ID moving forward

As we move forward techUK is committed to continuing to do its part. We will continue to convene the Industry and Government throughout the remainder of 2022 in our Digital ID Programme Working Group and 2022 Digital ID Event Series to provide the platform for us all to strive for the very best outcome for the UK Trust Framework.

techUK calls on the UK Government to work with us, our Members and all other key stakeholders to deliver on the clear recommendations and calls to action made in this report.

References

1. https://www.techuk.org/resource/digital-identities-the-missing-link-in-a-uk-digital-economy.html
2. https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version/uk-digital-identity-and-attributes-trust-framework-alpha-version-2
3. https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation,
4. https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation
5. https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation,
6. https://www.researchandmarkets.com/reports/5451239/global-digital-identity-market-2021-2027-by
7. https://www.gov.uk/government/publications/digital-identity-document-validation-technology-idvt/identity-document-validation-technology-in-the-right-to-work-and-right-to-rent-schemes-and-dbs-pre-employment-checking-accessible-version
8. https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation
9. https://digital.nhs.uk/news/2021/around-half-of-people-in-england-now-have-access-to-digital-healthcare
10. https://www.gov.uk/government/publications/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks/digital-identity-certification-for-right-to-work-right-to-rent-and-criminal-record-checks
11. https://hmlandregistry.blog.gov.uk/2021/03/12/setting-the-standards-for-identity/
12. https://www.gov.uk/guidance/using-the-eu-exit-id-document-check-app
13. https://www.ukauthority.com/articles/home-office-plans-generic-id-service/
14. https://www.gov.uk/government/publications/age-verification-technology-in-alcohol-sales-regulatory-sandbox#:~:text=The%20Home%20Office%20and%20Office,alcohol%20under%20the%20Licensing%20Act
15. https://www.pensionsdashboardsprogramme.org.uk/2022/02/07/pdp-appoints-digidentity-identity-service-supplier/#:~:text=On%20February%201%2C%202022%2C%20the,that%20will%20drive%20pensions%20dashboards.
16. https://www.gov.uk/government/news/new-legislation-set-to-make-digital-identities-more-trustworthy-and-secure
17. https://www.computerweekly.com/news/252496337/Government-to-impose-new-digital-identity-system-across-all-Govuk-services
18. https://www.computerweekly.com/news/252506595/UK-governments-new-digital-identity-system-to-cost-up-to-400m
19. https://bidstats.uk/tenders/2022/W07/76886856
20. https://bidstats.uk/tenders/?ntype=tender
21. https://gds.blog.gov.uk/2021/12/01/one-login-for-government-december-2021-update/
22. https://www.computerweekly.com/news/252506595/UK-governments-new-digital-identity-system-to-cost-up-to-400m
23. https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/digital/wp-call/2022/call-fiche_digital-2022-deploy-02_en.pdf, page 12 and Annexe 1
24. https://www.jmlsg.org.uk/guidance/
25. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth
26. https://governmentbusiness.co.uk/news/21032022/whitehall-cut-%C2%A355bn-wasteful-spending
27. https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/The-state-of-digital-identity-in-the-UK-such-a-great-idea-youll-need-a-whole-bunch-of-them
28. https://www.gov.uk/government/consultations/digital-identity-and-attributes-consultation/digital-identity-and-attributes-consultation

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