Verified

Policy Exchange

The UK's Digital Identity Dilemmas

Benjamin Barnard

Foreword by Matt Warman MP

Verified

The UK's Digital Identity Dilemmas

Benjamin Barnard

Foreword by Matt Warman MP

Policy Exchange

About the Author

Benjamin Barnard, Head of Technology Policy. Benjamin leads Policy Exchange's research into Technology and the Digital Economy. He joined Policy Exchange in July 2019 after graduating from Christ Church, Oxford with a First Class degree in History. He is the author of a number of reports including 'FinTech For All' (exploring how FinTech can improve access to financial services), 'Daylight Robbery' (detailing how to fight COVID-related public sector fraud) and 'Whitehall Reimagined' (which included recommendations to improve the use of technology and data across Whitehall).

Acknowledgements

The author of this report is thankful to all those who contributed to the research or who contributed through meetings and informal discussions. Specific thanks go to Will Heaven, Julia Mizen, Sophia Falkner, Gabriel Elefteriu, Dom Walsh, Frank Joshi, Joseph Spear, Ruth Milligan and Ross Kempsell for their input into this project. We would also like to thank a number of officials at the Department for Digital, Culture, Media and Sport, the Cabinet Office, the Government Digital Service and other Civil Service departments who have been helpful in providing information and responding to requests. Any errors remain the authors. Special thanks to Jos Henson-Grič, who started this report and who's contribution was invaluable

Published by
Policy Exchange, 8 – 10 Great George Street, Westminster, London SW1P 3AE

www.policyexchange.org.uk

ISBN: 978-1-913459-41-3

Contents

Foreword

Matt Warman MP

In these unprecedented times it has become more important than ever for businesses and the public sector to adapt quickly and provide people with services online. The need to prove who you are digitally has become a vital part of everyday life for many people.

We are an unashamedly pro-tech government and I was pleased to present, with Minister Lopez, the Government's response to the digital identity Call for Evidence in September. It was clear from all the responses we received that there is a lively public interest in the potential for an enabling framework of legislation, standards and oversight for digital identity.

Businesses want to be able to innovate and individuals are keen to quickly and easily access products and services relevant to them, confident they are protected from fraud and that robust privacy protections are in place. This new report from the Policy Exchange highlights the importance of considering all those elements as the digital identity market develops, and I welcome this timely contribution to the ongoing dialogue on digital identity.

I am particularly glad that the report acknowledges our responsibility as a society to ensure the digital transformation of our economy does not leave behind those who would not naturally choose to use new technologies. As our understanding of the possibilities of digital identity tools and products grows, I am inspired by the opportunities to provide solutions to the online problems regularly faced by some of the most vulnerable in our society.

Done right, digital identity can support inclusion, increase data privacy and control, and protect people from the increasing threat of cyber crime.

Our new National Data Strategy points to digital identity as a prime example of the kind of data-driven innovation that can - at the most practical level - spur on the digital transformation we are working towards across the entire economy.

As this report illustrates, there is much that both the government and the private sector can continue to build upon to create trust in digital identities.

This government is committed to increasing online security, delivering personalised services, increasing productivity and boosting the economy. It is committed to developing a cross-government identity system focused on user need. It is also committed to doing this without the need for ID cards. We are working at pace to realise this ambitious vision and continue to collaborate with industry and civil society groups to develop the next

phase of the digital identity economy.

This report makes a helpful contribution to the public debate which is vital as we work to create a secure, inclusive and fair framework that will enable products and services fit for the digital age.

Matt Warman MP, Minister for Digital Infrastructure

Executive Summary

The Importance of Identity

Every day we have to prove that we are who we say we are. When we buy alcohol, open a bank account or apply to receive benefits or entitlements, we have to produce physical documents (like passports, driving licences or utility bills) that contain private information about ourselves in order to prove our identity. Identity assurance is the first step in nearly all interactions between the government and its citizens, or between businesses and their customers.

Those without identity documentation will suffer from financial, economic and social exclusion. One in five people in the UK lack an "anchor" identity document, such as a passport or a driving licence. Without proof of identity, citizens will struggle to access basic services such as Universal Credit, will fail pre-employment checks (which require proof of address and the right to work in the UK) and will be unable to open a bank account, as Policy Exchange showed in *FinTech For All* (2020).

Identity proofing and verification is also vital in the prevention of, and the fight against, fraud. Fraud costs the UK economy at least £193 billion each year, equating to more than £6,000 lost per second every day. Moreover, as Policy Exchange demonstrated in *Daylight Robbery* (2020), the methods that fraudsters use to impersonate others become more advanced every year.

The Problem

As more services move online, customers and citizens now need to make assertions about their identity both digitally and remotely. This need has been highlighted by the COVID-19 crisis and the imposition of Government-mandated social distancing measures, which forced businesses and governments alike to complete identity checks digitally to avoid unnecessary face-to-face contact or the potential transmission of the virus via the handling of identity documents.

At present, proving one's identity online can be cumbersome and difficult. People often have to send scanned copies of their identity documents to organisations on the blind trust that their personal information will be stored securely and not misused, creating 'honey pots' of personal data for hackers. Moreover, customers have to manage hundreds of online accounts and constantly resubmit the same personal data every time they undertake an identity transaction, making it very difficult to

track which organisations are in possession of their personal information. Equally, even if people do submit accurate information about themselves, in the absence of a face-to-face check it is very difficult to prove that they are not fraudsters using personal information obtained from either cyber attacks or from data breaches in order to masquerade as another individual to gain unauthorised online access to goods, services or entitlements.

What is a Digital Identity?

Digital Identity schemes (or solutions) allow people to prove their identities online. A digital identity is a collection of data belonging to a legal entity which can be used as a digital representation of a unique person or organisation. A digital identity provides a method of electronically verifying that people are who they claim to be so that they can access services. Most digital ID transactions are actually based, initially, on physical documents or certificates, but, if you have a digital ID, you don't need to produce these documents to access online services. Such digital IDs are secured using advanced cryptographic techniques. Digital IDs can limit the amount of information that a user has to transfer to any organisation which relies on their identity assertion by confirming or denying whether that user meet the criteria rather than by transferring his or her personal information (such as their exact date of birth).

For organisations to have a high level of assurance in a digital ID, the data comprising a digital ID needs to be verified as accurate by trusted parties. Unless the data comprising a digital ID is verified as accurate by another party that is qualified to do so, then that digital ID cannot be used to access services that are sensitive to abuse by fraudulent actors. Once users have created 'verified' digital IDs, they can be used to access multiple services from multiple different organisations. Digital ID services that are designed with high user control allow citizens to control how their personal data is shared and who has access to it.

The Context to Digital ID in the UK

The UK differs from many European countries because it lacks a Government-mandated and centrally supported biometric ID card. Such cards often provide the basis of national digital ID schemes and can be used by citizens to access online services provided by both the public and the private sectors. The UK Government has a long-standing political commitment not to introduce biometric identity cards or establish a central database of citizen attributes, following the repeal of the Identity Card Act in 2011 (a decision taken in part on grounds of civil liberties). This is a unique foundational difference to other countries, such as Estonia, that have launched national digital identity programmes, many of which involve citizen biometrics. This report does not call for mandatory biometric ID cards supported by a centralised register of UK citizen attributes. Instead, it explores how to improve identity verification in the public and private sector.

Digital Identity in the Private Sector

The lack of reliable digital ID services is a severe limitation to the UK's digital infrastructure. At present, the UK is one of the world's leading digital economies. This progress will be hampered unless there are secure and reliable ways to prove one's identity when accessing goods and services online. To prevent fraud and to comply with regulations, businesses providing services online have to perform expensive, and often unreliable, checks on the information that their customers provide. Creating a viable digital ID ecosystem can help to prevent fraud across both the public and private sectors, as well as reducing administrative costs for businesses. Furthermore, digital vaccine certificates, stored in a decentralised way on users' phones and not on a central server, could possibly help to open up the economy once reliable COVID vaccinations are developed and widely available.

In the UK, the market for digital identity services is fragmented. The UK Government has a vital role to play in setting the regulatory standards and liabilities for digital ID services in the private sector. Likewise, the Government also has access to large data assets that could be used to verify the identities of those trying to access services provided by the private sector; it has a duty to protect consumers and offer them confidence in using digital identities. It must support the creation of a fully-functioning digital identity marketplace across both the public and private sectors, and one which which is recognized in the EU and internationally.

Digital Identity and Public Services

As more government services have moved online, Government Departments need to complete identity checks remotely and digitally. There are a number of public sector identity management systems. Every UK Citizen has an NHS number and can use NHS Login to access multiple digital health and social care services. Similarly, Government Gateway (run by HMRC) allows citizens to access over 120 Government services. The UK Government launched a common identity assurance platform called GOV.UK Verify in 2016 after a number of years in development. It was originally intended to replace Government Gateway and was launched with the aim of preventing multiple Government Departments from pursuing separate and siloed approaches to identity assurance, with the intention of reducing inefficiency and costs for taxpayers.

The Lessons Learnt from GOV.UK Verify

To avoid the creation of a government-held central register of UK citizen attributes, GOV.UK Verify took a 'federated' approach to digital ID. It outsourced the problems of verifying identity to a set of private companies or identity providers, known as 'certified companies', who each had to undergo checks to ensure that they could be trusted to keep user data secure. In order to create a Verify account, citizens choose to register with one of the certified companies and provide them with personal information which the companies then check against a variety

of different records. Once these checks are completed, you can use your Verify account to access Government services online such as to receive benefits (the Department of Work and Pensions was its largest customer) or to pay tax bills. In addition to providing identity assurance for the UK Government, GOV.UK Verify was also intended to create a market for digital IDs in the UK by encouraging citizens to create digital IDs which could then be reused in the private sector. GOV.UK Verify aimed to preserve user privacy by ensuring that the certified companies could not see which Government services their users were accessing and by preventing Government departments from seeing unnecessary personal information.

GOV.UK Verify has missed its targets. In 2019, both the National Audit Office and the Infrastructure and Projects Authority recommended that the Government terminate the project. The Government was supposed to stop funding the system (which has cost over £175m already) in April 2020 but, due to the surge in numbers of people claiming Universal Credit at the start of the COVID-19 crisis, HM Treasury agreed to provide GOV.UK Verify with public funds for a further 18 months, reportedly on the condition that the Government Digital Service (GDS) should not add any further Government services to the Verify roster. It also stipulated that GDS create alternative identity verification tools for services solely reliant on Verify. Furthermore, the Department for Work and Pensions has launched its own identity verification platform (Confirm Your Identity) and HMRC's *Government Gateway* was used to sign up Universal Credit claimants due to the strain on GOV.UK Verify during the COVID-19 crisis.

GOV.UK Verify struggled because it was launched before other Government Departments had promised to participate in the scheme. Moreover, its 'closed' commercial framework limited the number of third parties who could act as certified companies. Furthermore, the UK Government missed key opportunities to sign up others to the scheme, for which ministerial accountability was unclear. From the outset, it struggled to balance ease of access (ensuring that users managed to verify their identity in a quick and frictionless way) with the completion of the necessary and important tests that are required to prevent fraud. This resulted in poor user experience. It also did not make sufficient use of Government data sources during the identity proofing and verification process, which may have made it more difficult for certain demographics with weak digital footprints (known as "thin file" users) to sign up. This was a particular problem because the DWP was its largest customers and Universal Credit claimants were more likely than others to be "thin file" users.

The Future of Digital ID and Public Services

The UK Government needs to confront a number of separate, but related, dilemmas:

- **How to develop a reliable public sector identity model:** Unless the UK Government develops reliable identity solutions across Whitehall, there will always be a bottleneck on the development of the UK public sector's digital ambitions and a limited number of transactions between the Government and its citizens that can be completed online. Nonetheless, it must complete identity transactions in such a way that preserves the civil liberties and privacy of its citizens, a necessity that often generates controversy given the centrality of biometric data to many digital ID solutions in the private sector. The Government must determine the role of third parties in providing identity assurance for the Government and work out how to develop a secure and user-centric model of digital identity that puts individuals in control of their data.
- **'Siloes' or 'Platforms:'** The UK Government must determine whether it is possible to pursue a coordinated approach to digital ID across Whitehall, or whether it is instead preferable to encourage Government Departments to pursue individual (siloed) but tailored approaches to identity, in turn creating a suite of different identity solutions for different public services. Although there are clear advantages to developing a common approach, to do so will require political leadership and technical expertise to ensure that user experience is not compromised and that user needs are met.

Recommendations

- **Preserve traditional methods of identity checks.** Although this report aims to demonstrate the benefits of digital identity both as a way of preserving user privacy and of enabling better access to public services, there are many individuals who either lack the skills or resources to access services online or who may always feel uncomfortable creating and using a digital ID. Although there has been progress in addressing the digital divide in recent years, the Government should acknowledge this fact and ensure that there is never a situation in which having a digital ID is mandatory or that certain public services are only accessible through the creation and use of a digital identity. To do so will assuage any public concerns about digital ID policy and will also ensure that public services remain accessible to all.
- **Create a dedicated ministerial portfolio for digital identity.** Although the Government has announced the creation of a new Digital Identity Strategy Board, a dedicated minister for Digital Identity would ensure democratic accountability for Government identity policy.
- **Publish a 10-year Digital ID Strategy.** Such a strategy must clarify the future of GOV.UK Verify. It must also explore how biometrics are used in the wider private sector and set out how to protect consumers and their data in order to ensure that they are confident in using digital identities. It should also set out the long-term role of accredited third-party identity providers in the public sector. If third parties (such as banks) are to play a role in providing identification services to the Government, the strategy should explore how to establish a trust mark for digital identity products and the processes by which those trust marks are assessed.
- **The Department of Work and Pensions should continue to accelerate the launch of The Confirm Your Identity (CYI) service, which helps Universal Credit claimants prove their identity online during the application process.** The creation of a tailor-made identity solution for the DWP should be encouraged because those reliant on welfare are more likely to lack ID documentation. Nonetheless, there are clear advantages to developing cross-departmental identity solutions and there is a risk that every department will develop separate and siloed approaches to identity assurance, leading to increased costs for taxpayers. The development of a reliable cross-departmental identity solution that

is easy for citizens to use should be a key priority for Government.

- **Commence feasibility assessment for digital vaccination certification.** Once, and if, a vaccine for COVID-19 is developed, evidence that a citizen has received the immunisation through the official UK programme *could* be linked to a verified vaccination certificate, secured and stored in a decentralised and privacy-enhancing way on a user's phone. Although the Government is yet to outline its broader approach to vaccination, individuals could *possibly* use these verified vaccination certificates to gain access to a limited number of settings where the risk of infection is higher (such as a nightclub, for example) so as to ensure that the vulnerable are not exposed to the virus. The complexities and trade-offs associated with delivering such a scheme would be significant, including mitigating the risk of vaccine fraud. Scoping, consultation and feasibility assessment must, therefore, commence now.
- **Remove legislative barriers that prevent businesses from completing contactless identity transactions.** The UK Government should amend legislation (such as the Licensing Act 2003) that mandates private sector companies to check physical documents, so as to remove barriers to the use of digital identities. This will enable users to use digital IDs stored on their phones to prove their identity and prevent the risk of transmission of COVID through the handling of identity documents.
- **The Government should extend the scope of the Document Checking Service Pilot Scheme to include driving licences and increase participation in the scheme.** The Document Checking Service checks passport details against the HM Passport Office (HMPO) database. It provides a simple 'yes' or 'no' response to say whether a passport is valid without giving direct access to government-held data. The Government recently announced that they would be extending the DCS Pilot Scheme. In future, the number of private sector participants should be expanded dramatically, especially to include small and medium-sized enterprises (SMEs) and emerging FinTech companies. Furthermore, at present it is only possible to check passport data against HM Passport Office data. The service should be extended to check other identity documents including driving licenses.
- **Use the National Data Strategy to identify additional Government data sources that could be used to support identity proofing and verification processes.** To verify a person's identity, companies need to refer to a combination of official and commercially available data sources. This often happens by drawing upon data from Credit Reference Agency (CRA) files. The digital availability of Government registers (both to Government Departments and to private sector organisations) would support identity and eligibility checking. It could help to eliminate "thin

file" consumers who may struggle to access online services simply because they have weak financial or digital footprints**.** Like the document checking service, such data should be provided without giving direct access to government-held data.

- **Establish the regulatory requirements of the digital ID ecosystem.** Issues of liability will arise whenever a party suffers a financial loss as a result of a mistake made during the identity transaction process. The Government should establish regulations that stipulate who is liable for fraudulent use of a digital identity.
- **Establish more nuanced Digital ID standards across the public sector.** It is a complex challenge to find the balance between ease of access to services and the high levels of assurance that are often required to prevent fraudsters. The Government should establish more nuanced standards so that checks are not too rigorous and that there is not an abrupt cliff-edge between different levels of authentication that unnecessarily prevents people from gaining access to services.
- **Establish a Digital Business Identity programme.** This would could help to improve companies' access to government business support measures and make it easier to bid for Government contracts. It would also support those applying for grant funds and R&D Tax Credits.

Introduction

What is Digital Identity?

Every day we have to prove that we are who we say we are. When we buy alcohol, open a bank account, receive benefits or go through border controls, we have to produce physical documents (like passports, driving licences or utility bills) that contain private information about ourselves.[1] These documents can provide information including our age, our address, our nationality or for how long we have been resident in the UK. Even when we access services online, it is often still necessary to scan pictures of these physical identity documents, send them via post to Government agencies or business or go, in person, to be identified.

Digital IDs allow people to prove their identities online, without recourse to physical documents or artefacts. Put simply, a "digital identity" is a set of different pieces of information which can be used to identify a defined subject online (in this instance a person, but the same can be true of other legal entities such as businesses).[2] For example, by using a digital identity, somebody would be able to open a bank account without sending the bank a scan of their passport and their utilities bill to their bank. Most digital ID transactions are actually based, initially, on physical documents, but, if you have a digital ID, you don't need to produce these documents every time you complete a transaction.

What is a Digital Identity?

- A digital identity is a collection of data belonging to a claimed identity, usually verified by trusted parties, which can be used as a digital representation of a unique person or organisation.[3] The main role of a digital ID is authentication: to verify whether an entity is who (or what) they (or it) is believed to be and whether they are worthy of trust.
- The UK Government defines a digital identity as "a trusted way of proving one or more attributes about themselves online or offline and linking those attributes to that same person as a uniquely identifiable individual."[4]

1. GOV.UK, *Proof of Identity Checklist*, Updated 10 March 2014, https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist#proof-of-identity-checklist-for-individuals
2. TechUK, *The Case for Digital IDs*, 4 Feb 2019, https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf
3. OIX, *Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK: White Paper*, October 2019, https://openidentityexchange.org/wp-content/uploads/2019/10/Establishing-a-Trusted-Interoperable-Digital-Identity-Ecosystem-in-the-UK-White-Paper-Oct-2019.pdf
4. DCMS and Cabinet Office, *Digital Identity: Call for Evidence*, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf

When accessing services online (provided by either the public or private sector), it is very often necessary to prove that you are eligible. New technologies allow individuals and organisations to:

- Remotely verify original documents and extract data from them,
- Verify only selected data from documents (e.g. a name or age) rather than sharing all the included data,
- Perform binary verification checks of personal data without revealing personal details (for example, confirming whether somebody was over the age of 18, rather than revealing their date of birth)
- Control who has access to their personal information, provide greater transparency over who has access to that data and limit the amount of information being shared.

Why is digital ID vital to future UK prosperity?

Digital IDs are essential to the development of the digital economy. Any advanced economy (particularly one in which financial transactions are conducted digitally and vital services are accessed online) needs trustworthy and secure methods to provide businesses and citizens with the trust that they are dealing with real entities. That is why it is estimated that, by 2030, digital ID could create economic value equivalent to 6 percent of GDP in emerging economies and 3 percent in mature economies (on a per country basis).[5] By 2022, an estimated 60% of world GDP will be digitized, meaning that digital ID will be an essential tool in verifying the identities of parties involved in financial transactions and preventing fraud.[6]

The outbreak of COVID-19 has demonstrated the importance of digital ID. Government-mandated social distancing and the shift towards online services has demonstrated the urgent need for digital methods of proving one's identity. Indeed, the COVID-19 outbreak has meant that essential services, particularly those provided by the Government, that were previously administered face-to-face have had to be moved online. Ensuring that services are easily accessible to citizens whilst also ensuring that sufficient identity checks are completed in order to prevent fraudulent activity and unauthorised access to those services has been a complex challenge for Governments and businesses in the UK and abroad.[7] Industries, such as banking, which traditionally relied upon physical IDs to authenticate customers and employees have had to undergo a radical transformation to adapt to the conditions that COVID-19 has imposed on our lives to provide secure online services for their customers.[8]

5. McKinsey Global Institute, Digital Identification, A Key to Inclusive Growth, April 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx
6. TechUK, "FATF issues Guidelines on Digital ID", 7 April 2020, https://www.techuk.org/insights/news/item/17246-faft-issues-guidelines-on-digital-id
7. TechUK Event, *Now More than Ever*, 21 May 2020, https://www.techuk.org/insights/meeting-notes/item/17657-digital-identity-now-more-than-ever
8. Planet FinTech, *Digital Identity Verification 'on the rise' amid Coronavirus*, https://www.planet-fintech.com/Digital-Identity-Verification-on-the-rise-amid-Coronavirus_a1395.html

eIDAS

- eIDAS establishes mutual recognition of identity standards and provides a mechanism for permitting and forcing acceptance of eIDs authorised by one EU member state in all other member states.[9]

Digital IDs have a number of potential benefits. Although this paper will focus primarily upon the process of proving one's identity online, in addition to preventing cyber-crime and identity fraud, digital identity could also improve a range of private and public sector activities in the long-term (like credit rating or DRB checking) that rely on accurately linking individuals with information about them.[10][11] Digital identity could support a variety of different groups in the long-term:

- **Consumers:** increased security for, and control over, their personal data.
- **Government:** providing the tools for Government to engage with its citizens more efficiently and prevent fraud without greater encroachment on civil liberties.
- **Businesses:** a reduction in losses to fraud and the costs associated with regulatory compliance.
- **Society:** better and more efficient public services that deliver better value for money.

Other legal entities (such as corporations and trusts) also have to make assertions about their identity. Business to business (B2B) transactions depend upon the trust between parties. Moreover, many organisations need not only to let different employees access different internal services based on their attributes, but employees often need a mechanism to prove that they are, in fact, a representative of a legal organisation and that they have the authority to approve a commercial transaction or act on behalf of the company.

A Crucial Juncture: The UK's Digital Identity Dilemmas

The UK Government is at a crucial juncture when it comes to digital identity. Unlike many other countries, the UK Government does not have a state-issued biometric ID card upon which a public sector digital ID scheme could be based. Instead, there are a range of digital ID solutions across Whitehall, including HMRC's Government Gateway and GOV.UK Verify.[12] Indeed, GOV.UK Verify was launched with the intention of providing a single platform for all online identity transactions between the Government and its citizens, as well as to establish a digital ID market in the UK. [13] In May 2020, it was announced that GOV.UK Verify would be prohibited from adding additional services to its roster.[14]

10. Due to scope, this report will exclude digital ID in immigration and healthcare.
11. Seon, *"Digital ID Profiling and The Future of Credit Scoring", 12 March 2019*, https://seon.io/resources/digital-id-profiling-and-the-future-of-credit-scoring/
12. Government Digital Service, *Guidance*, "GOV.UK Verify", 18 June 2020, https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify; HMRC, *Corporate Report*, "HMRC Government Gateway Transformation Programme: Accounting Officer assessment summary", https://www.gov.uk/government/publications/accounting-officer-assessment-summary-for-the-government-gateway-transformation-programme/hmrc-government-gateway-transformation-programme-accounting-officer-assessment-summary
13. Hansard, *18th May 2011*, https://hansard.parliament.uk/Commons/2011-05-18/debates/11051863000014/IdentityAssurance
14. ComputerWeekly, *HM Treasury tells GDS: No further online services can use Gov.uk Verify, 7 May 2020*, https://www.computerweekly.com/news/252482828/HM-Treasury-tells-GDS-no-further-online-services-can-use-Govuk-Verify?_ga=2.34113895.758846749.1591016742-466382040.1591015386
9. Regulation (EU) No 910/2014 of The European Parliament And Of The Council of 23 July 2014

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

GOV.UK Verify

- GOV.UK Verify allows citizens to prove their identities online when accessing Government Services. It operates without a central government database of citizen attributes and works with certified companies, known as identity providers (IDPs), to prove users' identities.
- In order to create a Verify account you have to provide some personal information which is then checked against a variety of different records. Once these have been checked, you can use Verify to access Government services online such as the receipt of benefits or to pay tax bills.

The reported decision to discontinue GOV.UK Verify means that the UK Government is at a crossroads when it comes to identity policy. It needs to resolve the following questions:

- **Digital ID in the Private Sector:** What role should the UK Government play in regulating and supporting the UK digital ID market? What safeguards are necessary to protect citizens' information? Should private sector companies check government data sources for ID verification purposes to prevent fraud?
- **Digital ID in the Public Sector:** Multiple Government departments and agencies need to verify the identities of their citizens. Does the UK Government need to create a cross-departmental identity verification platform and, if so, what form should that take? What role should third party identity providers play in providing access to services provided by the public sector? How can the UK Government create identity assurance services that limit user friction and encourage ease of access whilst also ensuring that there are sufficient checks to prevent fraud?

How is this Report Structured?

This report is divided into three parts:

- **Core Concepts.** This part explains the theoretical model of how a digital ID service based on mutual standards and trust works, as well as the technology that enables it.
- **Digital ID in the Private Sector:** This section aims to show how digital IDs can support a range of public and private sector activities.
- **Digital ID in the Public Sector.** This part explores the state of the digital identity ecosystem in the United Kingdom. It explores the decisions that led to the creation of GOV.UK Verify and evaluates the performance of the programme.

Future UK prosperity is at risk unless it develops a viable digital ID ecosystem. The UK has historically been a world-leader when it comes to technological innovations.[15] Unless it acts now to facilitate the development of a digital identity market, it risks falling behind in this crucial digital frontier.

15. The Fletcher School, Tufts University, *Digital Evolution Index, 12 July 2017*,

https://sites.tufts.edu/digitalplanet/digital-evolution-index-the-uk-is-among-the-handful-of-digital-elite-countries-and-leader-of-europe-telecoms-tech-news/

Core Concepts

An Introduction to Digital ID

This chapter aims to explain the core concepts behind digital identity. It is divided into four sections. These are:

1. Traditional Identity Verification
2. Defining Digital Identity
3. Standards and Trust
4. Identity Verification Technology

Traditional Identity Verification

In the United Kingdom, citizens use a range of physical documentation to prove their identity. Issued by a range of different Government Departments and organisations, both the Government and private businesses use these documents to check the identities of their citizens and customers (respectively).[16] They do so to check that they are eligible to receive entitlements, to comply with regulations (such as age restrictions or anti-money laundering measures) and to mitigate the risk of fraud.[17] All of these documents contain different pieces of personal information, which can be used to prove our identity.[18] These forms of identity include, but are not limited to:

- Bank statements
- Birth certificates
- Driving Licences
- National Insurance Numbers
- Passports
- Residence permits
- Tenancy agreements
- Tax documents – such as P45s and P60s
- Utility bills

Traditionally, these documents have been checked manually. Checks are undertaken to determine whether people are presenting fake IDs and, if the ID is legitimate, that it doesn't belong to somebody else. This process can be time-consuming, inconvenient and expensive for businesses. Moreover, without specialist tools, it is often difficult to detect fraudulent documents. Those without any identity documentation whatsoever will

16. Cabinet Office & Department of Culture, Media and Sport, *Identity proofing and verification of an individual*, 17 December 2019, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/identity-proofing-and-verification-of-an-individual

17. FinTech Futures, *The Future of Client Onboarding, 24 September 2019*, https://www.fintechfutures.com/2018/09/the-future-of-client-onboarding/

18. The Money Laundering and Terrorist Financing (Amendment) Regulations 2019, http://www.legislation.gov.uk/uksi/2019/1511/contents/made,

CIMA Global, https://www.cimaglobal.com/Global/UK/AML%20statutory%20instruments.pdf,

struggle to access essential Government services and will not be able to open a bank account.[19]

ID Documents and Social Exclusion

Lack of ID is a key driver of financial and social exclusion. Many individuals (known as 'thin file' individuals) may be denied access to essential services:

- Those who lack proof of their identity are unable to open bank accounts and will struggle to access Government entitlements and benefits, such as Universal Credit. As Policy Exchange pointed out in *FinTech for All*, those who are unable financial services will suffer from severe social exclusion.[20]
- They are also likely to fail pre-employment checks, which require proof of address and the right to work in the UK to be confirmed.[21]

Many in the UK, and globally, lack ID documents:

- One in five of the UK population has no root anchor document, such as a passport or driving licence.[22]
- 1 billion people globally are recognised to lack any form of digital ID.[23]

Defining Digital Identity

As more and more services move online, it is now necessary to prove your identity digitally and remotely. Individuals often have to create multiple accounts with different organisations to create a unique credential (often, a username and password) for every online service they access to prove that they are who they say they are.[24] The average person manages in excess of 191 pairs of usernames and passwords.[25] Not only is this unmanageable and insecure, but it also places a great burden on organisations to verify their customers' identities and ensure that their data is secure.[26] Worse still, they often have to scan physical documents and transfer them, often insecurely, to parties relying on their identity assertions in the blind trust that these organizations will not lose or share their data without their permission. Although there are a number of different regulatory requirements on businesses and Governments to protect their citizens' data (such as those set out in the Data Protection Act 2018), there is no guarantee that companies or governments themselves will handle personal data properly.[27]

19. Policy Exchange, FinTech for All, January 2020, https://policyexchange.org.uk/publication/fintech-for-all/
24. Virginia Tech, "The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services", https://people.cs.vt.edu/gangwang/pass.pdf
25. Security Magazine, Average Business User Has 191 Passwords, 6 November 2019, https://www.securitymagazine.com/gdpr-policy?url=https%3A%2F%2Fwww.securitymagazine.com%2Farticles%2F88475-average-business-user-has-191-passwords
26. As you can provide a false name and other information on sign-up, such accounts are "unverified" digital identities. As a result, without further checks, they can't be used to access vital public services or be used to complete transactions where there is a high risk of fraud.
27. Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
20. Experian, *Making the Invisible Visible*, https://www.experian.co.uk/assets/consumer-credit-risk/making-the-invisible-visible.pdf
21. NARCO, "*Lack of valid ID identified as key barrier t moving on from crime*", 21 November 2018, https://www.nacro.org.uk/news/nacro-news/lack-of-valid-id-identified-as-key-barrier-to-moving-on-from-crime/
22. Tech UK, *The case for digital IDs*, February 2019 https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf
23. World Economic Forum, *What does a Good Digital ID look like?*, 7 May 2019, https://www.weforum.org/agenda/2019/05/what-does-a-good-digital-id-look-like/

GDPR and the Data Protection Act 2018

- The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).[28]
- The UK implemented the General Data Protection Regulation (GDPR) through The Data Protection Act 2018.[29]
- According to research, the introduction of GDPR led to a $3.38 million decrease in the aggregate dollars raised by EU ventures per state per crude industry category per week, a 17.6% reduction in the number of weekly venture deals, and a 39.6% decrease in the amount raised in an average deal.[30]

A digital ID can be used to prove an individual's identity and their right to access information or services *online*. The difference between digital IDs and physical IDs is that a digital ID can be authenticated both remotely and digitally. Once created, digital IDs can be reused multiple times to access multiple different services, preventing the need to resubmit personal information. They can combine multiple types of high-fidelity digital data, as well as the personal information contained in the identity documents above.[31]

Verified and Unverified Digital IDs

- **Verified digital identities** are made up of verified (confirmed) attributes – proof that someone is who they say they are – from documents such as passports, driving licenses, birth certificates and biometric scans. Once this identity is created it can be used like a passport around the web to access a whole range of other services.
- **Unverified digital identities** are created when people register on websites with their name, date of birth and other personal details. This is still a form of digital identity (although some would argue that it was not), which will allow access to other services (for example, you can sign up to some other websites using your Facebook/ Google account) but there are many duplicates and fake profiles set up on some sites. This would not be possible with a verified digital identity, which is why you are unable to use unverified identities to access government services and banking services, for example.[32]

Digital IDs have a number of different uses. These include:

- Overcoming the difficulties of proving your identity online
- Providing a mechanism to delegate authority and act on behalf of another individual (such as an elderly or vulnerable member of family).
- Providing a mechanism to prove that you have the authority to act on behalf of an organisation (if, for example, you are a company director).

31. Mastercard, *Restoring Trust in a Digital World*, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf
28. General Data Protection Regulation (GDPR), https://gdpr-info.eu
29. Data Protection Act 2018, http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
30. Truth on the Market, "*GDPR After One Year: Costs and Unintended Consequences*", 24 May 2019, https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/
32. YOTI, *Digital Identity Toolkit Section 3: Digital identity explained*, 1 January 2010, *https://www.yoti.com/wp-content/uploads/2020/01/Digital-Identity-Toolkit_Section-3_Digital-identity-explained.pdf*

- Preventing the need for organisations to store copies of our personal data, thereby reducing the risk of fraud and also preventing the loss of sensitive data if services are breached,
- Reducing costs of businesses who have to complete due diligence on their customers,
- Making it easier to reclaim an identity after being the victim of identity theft.

Digital IDs have the potential to be used to do more than make identity assertions. Crucially, once a citizen has created a digital ID relating to themselves, it is possible to link more information and data to that verified identity. In the long-term, digital ID provides a mechanism of storing data from multiple sources - from both the private sector and from the public sector - and giving individuals the capacity to control how their digital IDs are used.[33]

Many countries around the world have digital identity services or schemes for their citizens.[34] These schemes or services provide a mechanism for customers to share their identity attributes with third parties to access a product or service online.[35] Although digital ID services have high start-up costs, and are complex to create, once created they can operate at low costs and have the capacity to protect user privacy.[36] These schemes are particularly effective when they are interoperable across both the public and private sectors, as they can prevent different organisations from pursuing siloed and incompatible solutions to digital ID problems.[37]

Digital ID Data

Digital IDs encompass a wide range of data about individuals. Knowing that someone is who they say they are, to an appropriate level of certainty for the task in hand, is complex and changes over both time and context. Digital Identity can be more than just "a digitized passport, driver's license, or national ID card, a password replacement or an online profile".[38] Instead, digital identity is:

> *"grounded in a collage of data that defines the individual. This collage of data, when bound to the individual, verified, and made securely accessible while under a user's control, is the essence of digital identity. Its primary purpose is not just to identify somebody, but more importantly to confirm their entitlement to access a service or perform a particular task."*[39]

33. House of Commons, Science and Technology Committee, *Digital Government*, 3 July 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1455/1455.pdf See "Self-Sovereign" Identity below.
34. See Chapter 3
35. OIX, *Cost of doing nothing*, April 2018, https://openidentityexchange.org/blog/2018/04/19/cost-of-doing-nothing/
36. OIX, *Cost of doing nothing*, April 2018, https://openidentityexchange.org/blog/2018/04/19/cost-of-doing-nothing/
37. OIX, Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK October 2019, https://openidentityexchange.org/blog/2019/10/04/establishing-a-trusted-interoperable-digital-identity-ecosystem-in-the-uk/
38. Mastercard, Restoring Trust in a Digital World, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf
39. Mastercard, Restoring Trust in a Digital World, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

Different types of data that can make up a digital identity

Digital IDs include a wide variety of different types of data.[40] These include:

- **General Data:** name, date of birth, address.
- **Biometric Data:** such as a fingerprint, facial or vocal records or iris scans.
- **Attribute Data:** such as a passport number, a national insurance number or an NHS number.
- **Certification Data:** such as a university degree, a driving license or a workplace qualification.
- **Dynamic Data:** this is data generated from online interactions with, for example, financial institutions, retail stores, mobile networks or Governments.

These different attributes can come from a range of sources, including but in no way limited to:

- Bank accounts
- Credit scores
- Personal devices
- Licenses
- Digital footprints
- Medical records

When completing identity checks online, it is essential to obtain 'genuine presence' assurance. It is essential to ensure that accurate personal information isn't being used by an impersonator to gain access to services. Checks have to be completed to ensure that the person submitting the information is real (and that they are not using photos or masks to gain unauthorised access) and that they are present at the time of the transaction (thereby ensuring that fraudsters are not using a video of a previous authentication to gain access).[41] This can make digital ID schemes controversial on civil liberties grounds, due to the fact that "biometrics (such as fingerprint or iris scans) are increasingly used as an identification method, from national e-ID initiatives to identifying the correct use of a mobile phone or tablet to allow access."[42]

41. IProov.com *The FCA coronavirus letter explained: how to remotely onboard customers without encouraging criminals, 1 April 2020.* ihttps://www.iproov.com/news-room/blog/the-fca-coronavirus-letter-explained-how-to-remotely-onboard-customers-without-encouraging-criminals

42. YOTI, *Digital Identity Toolkit Section 3: Digital identity explained*, 1 January 2010, *https://www.yoti.com/wp-content/uploads/2020/01/Digital-Identity-Toolkit_Section-3_Digital-identity-explained.pdf*

40. Mastercard, Restoring Trust in a Digital World, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf

Different Levels of Assurance

What makes a good Digital ID?

- **Verified and authenticated according to a high degree of assurance:** The standards for initial registration and subsequent acceptance of identity verification are set high.
- **Unique:** an individual or business has only one identity within a system, and every system identity corresponds to only one individual.
- **Private:** Digital IDs should give users access to their personal data, control over which other parties have access to their data and transparency as to who has accessed their data.
- **Consent-based:** individuals knowingly register for and use the digital ID with knowledge of what personal data will be captured and how they will be used.
- **Reusable:** individuals can use their digital IDs to ensure access to multiple services, ideally across both the private and public sectors.

There are differing levels of assurance that you can have in a digital identity. The Government Digital Service's *Good Practice Guide (GPG)* for Identity Proofing and Verification of an Individual identifies 5 different elements that need to be checked to prevent fraud:[43]

- **Strength:** get evidence of the claimed identity
- **Validity:** check the evidence is genuine or valid
- **Activity:** check the claimed identity has existed over time
- **Identity Fraud:** check if the claimed identity is at high risk of identity fraud
- **Verification:** check that the identity belongs to the person who's claiming it.

After all five of these checks have been undertaken, it is then possible to assign users to an identity profile. There are four different identity profiles to which you can be assigned, relating to different levels of confidence. The higher the risk of an identity-related crime, the higher the level of assurance is necessary.[44]

- low confidence (previously known as 'identity level 1')
- medium confidence (previously known as 'identity level 2')
- high confidence (previously known as 'identity level 3')
- very high confidence (previously known as 'identity level 4')

43. Cabinet Office and GDS, *Identity proofing and verification of an individual*, 11 September 2015, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

44. Cabinet Office and GDS, *Identity proofing and verification of an individual*, 11 September 2015, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

'Portable' Digital Identities

Bring Your Own Identity (BYOI)

Bring your own identity (BYOI) is the concept of allowing users to select and use a digital ID which they alone control to access multiple digital services.

'Portable' digital identities allow people to re-use their verified identity to access services so that they don't need to be re-verified every time they want to access new services. 'Portable' Digital IDs are based on the trust that when individuals create a digital ID, they do so in compliance with an agreed set of standards. These standards ensure that organisations undertaking checks can determine the strength of digital identities by grading the types of evidence and the methods of checking identities.[45] The trust that these standards are being observed is essential to digital identity, to quote Mastercard:

> *"Digital identity is about establishing that confidence and trust at both ends of the interaction. Each party needs to be confident that the party at the other end is who they say they are. And both require trust in the system that mediates that interaction."*[46]

Standards and Interoperability

In order for digital IDs to be 'portable', they need to be created in accordance with common standards that can be recognised both domestically and internationally. There are a number of advantages to a standards-based approach:

- Standards allow companies that rely upon digital identities to be sure that identity assertions are of sufficient quality to prevent fraud, preventing them from having to complete their own (often expensive) checks on customers and be sure that the digital identities they rely on are sufficient to meet regulatory requirements.[47]
- Standards allow users to re-use their digital identities across both the public and private sectors and also encourage interoperability across borders between national identity schemes with similar standards.[48]
- Allows regulators of different industries (e.g. gambling or financial services) to set their own identity assurance requirements against recognised standards.[49]
- Prevents users from having to continually go through the verification process each time they encounter a new organisation that relies upon their identity assertion.[50]

45. ID Crowd, *Why we need standards based digital identity*, 19 November 2018, http://idcrowd.co.uk/home/stds/
46. Mastercard, *Restoring Trust in a Digital World*, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf
47. ID Crowd, *Why we need standards based digital identity*, 19 November 2018, http://idcrowd.co.uk/home/stds/
48. OIX, Establishing a Trusted Interoperable Digital Identity Ecosystem in the UK October 2019, https://openidentityexchange.org/blog/2019/10/04/establishing-a-trusted-interoperable-digital-identity-ecosystem-in-the-uk/
49. ID Crowd, *Why we need standards based digital identity*, 19 November 2018, http://idcrowd.co.uk/home/stds/
50. OIX, The value of digital identity to the financial service sector, December 2016, https://openidentityexchange.org/wp-content/uploads/2017/01/The-value-of-digital-identity-to-the-financial-service-sector-Full.pdf

Roles in the digital ID ecosystem

There are a number of different roles in the digital identity ecosystem.[51] These include:

- **Users:** users make assertions about their identity to access services online. For example, if I tried to buy alcohol online, I would assert that I was old enough to do so.
- **Relying Parties:** Relying parties depend upon the identity assertion of the user. To continue the example, the company selling me alcohol would be the relying party.
- **Identity Verification Providers (also known as Attribute Providers):** These are organisations that verify different aspects of a user identity assertion. For example, a university could act as a verification provider by verifying that its graduates were qualified to practice in certain professions such as the law or medicine.
- **Identity Providers (also known as Trust Providers):** They provide the tools and the service connectivity for the user.
- **Identity Hubs (also known as Identity Service Providers):** Responsible for the service orchestration, the commercial framework through which participants are paid and the standards of identity assurance.

It is important to note that some system participants may play more than one role. For example, a bank might act as both a trust provider and an identity verification provider. A bank may also rely upon a verified identity as a relying party when onboarding customers. Similarly, a government may also play a number of different roles, particularly across departments. For example, a government's passport office may act as an identity verification provider, its health service may be a relying party and this whole process may be orchestrated by the government's digital identity service. Nonetheless, the advantage of such a system is that the organisations playing different roles cannot see what service a user is trying to access. This helps to ensure user privacy.[52] In order to encourage people to play their different roles, there has to be a commercial framework to provide incentives for businesses to provide the tools and identity verification checks. This means that relying parties can pay when they need to check users' identity according to rates established by the identity service provider.

The key advantage to an identity ecosystem with competing identity providers is that it avoids the need to create a single central register of identity attributes. A market of competing identity/trust providers prevent the need to create a new single central repository of collated information and personal data. Securing such high profile 'goldmines' of personal data is not only costly and technically difficult, but provides a clear target for hackers to attack and significantly increases the risk that a massive data breach will occur at some point, such as that which happened in South Korea in 2014.[53]

51. Mastercard, Restoring Trust in a Digital World, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf
52. Mastercard, Restoring Trust in a Digital World, March 2019, https://www.mastercard.us/content/dam/mccom/en-us/issuers/digital-identity/digital-identity-restoring-trust-in-a-digital-world-final-share-corrected.pdf
53. JapanTimes, 4 October 2014, https://www.japantimes.co.jp/news/2014/10/17/business/tech/theft-data-belonging-millions-south-koreans-forces-id-system-overhaul/#.XFMSps_7RTY

South Korean Data Breach (2014)

- In 2014, South Korea's national identity number computer system, which held the ID codes for 80 per cent of the population, was hacked.
- Each South Korean citizen had been issued with a lifetime unique ID number, which they used all transactions. This system had been in place since the late 1960s.

Identity Verification Technology

Identity document validation technologies (IDVT) provide the foundations for standards-based digital ID ecosystem. There are three main purposes to these technologies:

- **Authentication:** They confirm that the documents provided by a customer are not forged and that they are authentic.
- **Validation:** They confirm that an identity document hasn't been stolen or that it hasn't expired.
- **User Assurance:** They confirm that an identity document relates to the holder and that the person trying to access services isn't using documentation relating to others.[54]

Different types of Identity Verification Technology

IDVTs usually consist of:

- **Scanning Devices:** to scan an identity document or take a photograph to sufficiently high standard.[55]
- **Optical character recognition (OCR) software:** such software converts images of the text on an identity document into machine-encoded text, which allows the details it contains to be checked against records.[56]
- **Templates library of identity documents:** these templates can be used to check the security features on submitted identity documents and compare their contents against templates stored in a library in order to determine whether the identity document is authentic.[57]
- **Access to other datasets:** IDVTs must be able to make checks against other databases, such as Interpol's lost and stolen passport data, to ensure that identity documents are valid. This is done in the UK by the document checking service.[58]
- **Near Field Communication (NFC):** the NFC readers in smartphones can be used to transmit passport information in a secure way directly from the Near Field Communication (NFC) chip embedded in e-passports.[59]

Smartphones contain the hardware to allow for many of these functions. Indeed, the possibility of remote verification of identity documents has

54. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
55. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
56. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
57. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
58. Home Office, 'Identification Document Validation Technology', 28 March 2018, link
59. NFC technology was used most notably to support the Home Office's Settled Status Scheme.

only recently been made a reality due to the relatively recent proliferation of smartphones. Indeed, Smartphones now include high definition digital cameras and biometric sensors (used for facial recognition and fingerprint scanning), as well as a microphone (which can be used to capturing audio samples from users).

'Decentralised' Identity Wallets

A number of businesses, who want to act as identity providers, are developing a secure digital identity 'wallets'. These wallets are created by users via an app on their smartphone device. This wallet is an empty container at first. To be useful as a means of identity verification, it must collect and verify traditional identity documents from the user. For example, a user can scan their passport on their smartphone. The smartphone camera can be used to check the numerous security features, such as holographs and watermarks, with an increasingly high degree of accuracy. Similarly, biometric data and audio recordings, as well as a current photograph of the user, can all be captured via an app on a smartphone. Nonetheless, unless the data submitted is verified against other sources of data, to a set of agreed standards (such as those above), such systems can only facilitate self-assertion of identity and cannot be used to provide access to services sensitive to fraud.

This information is then stored securely. Each piece of data is individually encrypted and then stored separately within a digital identity wallet, protected by its cryptographically secured file storage system. At its most advanced, these encrypted files could be stored on individual devices – in a decentralised way - preventing the need for user data to be stored central servers, thereby preventing the creation of a "honey pot" of identity data. Furthermore, whereas anybody could steal an identity document, digital identity wallets give people the ability to 'unlock' and 'decrypt' their own digital identity wallet. This means that in order to access a digital ID wallet (a precursor to sharing their documents), you would have to present some form of biometric data and demonstrate sole knowledge of the unique private decryption key for your data.

Multi Factor Authentication

The security of digital ID systems can be enhanced through multi-factor authentication. Multi-factor authentication ensures that computer users are granted access only after successfully presenting two or more pieces of evidence (or factors) about themselves.

This can be used by people to assert their identity. For example, when entering a nightclub, a user would traditionally have had to carry a physical document. By contrast, those using a digital ID wallet could gain access without revealing any personal data by allowing the club to perform a "YES/NO" scan of their unique QR code within the app. Such a system facilitates a more secure way of data sharing because at no point is the customer's data 'transferred' to the business or person that needs to verify a customer's identity.

Case Study: Yoti

Founded in 2014 by Robin Tombs, Yoti now has over 200 employees, more than 5 million users and a 2019 market valuation of £82m.[60] Yoti is a secure digital identity app, that enables people to verify and securely store a range of official documents and personal information in one place on their phone.[61] The app allows people to securely share and utilise their documents and personal data, in a variety of different ways that are appropriate to the type of verification checks they needed to pass and the information asked of them by a person, business or government agency.

Yoti's digital identity service can be broken down as follows:

- Verification of existing identity documents and personal data
- Secure storage and encryption of a person's data within a Yoti 'wallet'
- Verification processes that allow users to securely authenticate their identity or details
- Secure data transfer connections that allow personal data to be sent and received
- Verification of existing identity documents and personal data

Yoti is by no means the only company offering a secure encrypted digital identity system and accompanying 'wallet' app.[62] Many other companies allow users not only to store but also share their personal data and identity documents.

Digital ID wallets allow users to control access to their data with real time control. In cases where access to personal information is required, digital ID wallets allow users to control their data by giving users the capacity to grant and revoke access to their personal information rather than transferring their data.[63] Some systems have already been pioneered in countries like Estonia.[64] Nonetheless, it is important to remember that whilst they may offer users high degrees of control over their digital identities, many e-id systems are, nonetheless, based on identity cards and a centralised citizen attribute registry.[65]

DLT and The Future of Digital ID

Distributed Ledger Technology (DLT) has the potential to transform digital identity. Whilst DLT Digital ID systems are not presently feasible, they may well be in the future.[66] DLT could address many potential issues around digital identity at present. It could ensure that Digital IDs cannot be replicated, that the files could be tamper proof and that people can control their own identities, paving the way for self-sovereign identity.[67]

63. https://institute.global/policy/new-approach-digital-identity
64. E-estonia, https://e-estonia.com/
65. E-estonia, https://e-estonia.com/
66. OIX, *Self-Sovereign & Shared Ledgers – A New Dawn for Digital Identity*, April 2019, https://openidentityexchange.org/blog/2019/05/14/self-sovereign-shared-ledgers-a-new-dawn-for-digital-identity/
67. Finextra, *KYC and Blockchain*, 30 March 2017, https://www.finextra.com/blogposting/13903/kyc-and-blockchain;

https://openidentityexchange.org/wp-content/uploads/2019/06/Self-Sovereign-and-Shared-Ledgers-Innovate-Identity-Jan-2019.pdf

60. TechCrunch, 2 August 2019, https://tcrn.ch/2IbSf6J
61. YOTI, *Prove My Age Whitepaper*, April 2019, https://www.yoti.com/wp-content/uploads/2019/06/PMA-white-paper.pdf
62. https://bloom.co; https://global.id; https://folio.id/

Self-Sovereign Identity

- DLT provides a route to developing a digital self-sovereign identity system, which gives individuals as much control over their data in terms of use, ownership and collation.[68]
- Self-sovereign identity envisions consumers and businesses eventually taking control of their identifying information on electronic devices and online, enabling them to provide validation of credentials without relying on any central repository be it held by social networks, banking institutions or government agencies.[69]

68. **Computerworld,** *How blockchain makes self-sovereign identities possible, 10 January2018* https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html

69. **Sovrin,** *What is self-sovereign Identity?*, **6 December 2018** https://sovrin.org/faq/what-is-self-sovereign-identity/

Digital Identity in the Private Sector

The Building Blocks of a Digital Economy

This chapter will explain why Digital IDs are crucial to the UK's digital future. As Tech UK rightly points out, digital identity has a wide-range of potential applications, ranging from onboarding customers to financial services to registering drones and devices connected to the Internet of Things (IOT).[70] This chapter seeks to draw upon a few examples to show why the UK Government should make digital ID one of its top priorities. Unless it does so it risks falling behind in this crucial digital frontier, thereby hampering the UK's future economic prosperity, digital development and global role in setting privacy standards. Creating a viable digital ID ecosystem can help to prevent fraud across both the public and private sector, as well as reducing administrative costs for businesses.[71] If the technology is widely adopted, it is estimated that, by 2030, digital ID could create economic value equivalent to 6 percent of GDP in emerging economies and 3 percent in mature economies (on a per country basis).[72] Other estimates suggest that Digital ID can contribute in excess of £58 billion in potential value to the UK economy specifically.[73]

Improving Know Your Customer (KYC) Procedures and Preventing Fraud

Secure and trustworthy identity verification processes are vital to businesses. CTRL-Shift estimate that the total costs of identity assurance processes in the UK exceed £3.3bn.[74] According to a survey conducted by Telesign, 82% of companies struggle with fake users and 52% of online companies do not have a formal process for verifying the identities of their customers online at first registration.[75] Indeed, the same study showed that although 75% of companies didn't believe that usernames and passwords provided a sufficiently secure authentication method for their users, 94% of companies used password or pins to create an account.[76]

Digital IDs provide a more efficient way of conducting 'Know Your Customer' (KYC) procedures. This refers to the process by which companies verify the identity and financial conditions of customers before doing business with them.[77] There is a multiplicity of private companies offering these services including iProov, Trulioo, Onfido and Au10ix.[78]

70. Tech UK, *Digital Identity - Let's Just Do It, 13th February 2020* https://www.techuk.org/insights/event-round-ups/item/16813-digital-id-lets-just-do-it
71. OIX, Cost of doing nothing, April 2018, https://oixuk.org/wp-content/uploads/2018/04/Cost-of-Doing-Nothing-FINAL3v3b.pdf
72. McKinsey Global Institute, *Digital Identification, A Key to Inclusive Growth*, April 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx
73. OIX, Cost of doing nothing, April 2018, https://oixuk.org/wp-content/uploads/2018/04/Cost-of-Doing-Nothing-FINAL3v3b.pdf
74. CNTRL-SHIFT, *Economics of Identity, October 2014*, https://www.ctrl-shift.co.uk/wp-content/uploads/2014/06/Ctrl-Shift-and-OIX-Economics-of-Identity.pdf
75. Telesign, *The Fraud Report: How Fake Users Are Impacting Business*, November 2015, link
76. Telesign, *The Fraud Report: How Fake Users Are Impacting Business*, November 2015, link
77. AFI, *KYC Innovations, Financial Inclusion and Integrity, March 2019*,

https://www.afi-global.org/sites/default/files/publications/2019-03/KYC-Innovations-Financial-Inclusion-Integrity-Selected-AFI-Member-Countries_0.pdf

78. Trulioo, https://www.trulioo.com/; Authentix, https://authentix.com/ Onfido, https://onfido.com/

Ensuring that customers are properly identified is not only vital to the prevention of late payment and corporate fraud but also a process for safeguarding competitive advantages. Companies that do not properly identify their customers not only run the risk of regulatory fines but can also damage their business schedules, reputations and cash flows.[79]

Electronic Signature

- Many electronic identity services also give users the option to sign electronic documents with a digital signature.
- This type of signature provides the same legal standing as a handwritten signature as long as it adheres to specific regulatory requirements

Digital identity is critical to tackling and preventing the proliferation of online fraud. Fraud costs the UK economy £193 billion a year.[80] Indeed, according to CIFAS data, there was a 6% increase in fraud from 2017 to 2018, with identity fraud growing at an even faster rate, increasing by 8% over the same period.[81] According to the University of Portsmouth's annual fraudscape report, in 19 out of every 20 instances of identity fraud, it is the victim who is left to pick up the pieces after a fraudster has used his/her name to apply for products and services.[82] The reason for the increase in online fraud and economic crime is that there is a growing online marketplace for identity documents on the dark web. Stolen personal identifiable information (PII) can be obtained from cyber attacks.[83] This can allow fraudsters to invent synthetic identities, in which a criminal combines real and fake information to create a new identity, or to take over real identities to commit fraud.[84]

79. FCA, *Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)*, https://www.handbook.fca.org.uk/handbook/FCG.pdf
80. Portsmouth University, *Annual Fraud Indicator*, link
81. CIFAS, *Fraud continues 'inexorable' rise in the UK as new annual figures show 6% increase*, 21 June 2019, https://www.cifas.org.uk/newsroom/fraudscape-2019-release
82. Portsmouth university, *Annual Fraud Indicator*, link
83. Fraud Magazine, April 2014, https://www.fraud-magazine.com/article.aspx-?id=4294982013, HBS Digital Initiative, *The Growing Market for Identifying Fake IDs*, 13 November 2018, https://digital.hbs.edu/platform-rctom/submission/the-growing-market-for-identifying-fake-ids/
84. ID Crowd, *Why we need standards based digital identity*, 19 November 2018, http://idcrowd.co.uk/home/stds/

Types of Identity Fraud

True (Traditional) Identity Fraud: this is the simplest type of fraud and implies the stealing or purchasing of a victim's identity details (or credit card or payment details) on the Dark Web.

Synthetic Identity Fraud. There is a growing online marketplace for identity documents on the dark web. Stolen personal identifiable information (PII) can be obtained from cyber attacks.[85] This can allow fraudsters to invent synthetic identities, in which a criminal combines real and fake information to create a new identity, or to take over real identities to commit fraud.[86] There are two methods used by fraudsters to create synthetic identities:

- **Manipulated Synthetics** are based on a real identity and only limited changes are made to the identity, usually to hide previous history.
- **Manufactured Synthetics:** are composed of valid data assembled from multiple identities. They are often referred to as 'Frankenstein' identities because fraudsters cobble together bits and pieces of personally identifiable information (PII) from real people to create fake identities.

Policy Exchange showed in *Daylight Robbery* that the Coronavirus crisis and the unprecedented economic interventions from the UK Government may result in £4.8bn of costs in fraud and error.[87] Digital IDs would help to prevent identity fraud and to help both Governments and Private Sector companies to prevent fraudsters using manipulated and manufactured synthetics to commit fraud.

Customer Onboarding in Financial Services

Digital identity is of particular importance to financial institutions because of the regulatory and anti-money laundering regulations that apply to them. Unless people can prove their identity they will be unable to open a bank account. As Policy Exchange pointed out in *FinTech For All* a lack of identity documents is one of the key drivers of financial exclusion.[88] Digital IDs will help financial institutions become more financially inclusive by:

- Making it easier for "thin file" customers to open bank accounts,
- Making the process of "onboarding" (the process which users go through when they start their journey as a customer/client of a bank/financial institution) new customers easier and cheaper,
- Improving credit scoring by providing lenders with the tools to more accurately evaluate consumer credit history. This, in turn, can decrease the overall cost of lending.

87. Policy Exchange, *Daylight Robbery*, 11 July 2020, https://policyexchange.org.uk/publication/daylight-robbery/
88. Policy Exchange, FinTech for All, January 2020, https://policyexchange.org.uk/publication/fintech-for-all/
85. **Fraud Magazine, April 2014,** https://www.fraud-magazine.com/article.aspx-?id=4294982013, **HBS Digital Initiative,** *The Growing Market for Identifying Fake IDs*, **13 November 2018,** https://digital.hbs.edu/platform-rctom/submission/the-growing-market-for-identifying-fake-ids/
86. **ID Crowd,** *Why we need standards based digital identity*, **19 November 2018,** http://idcrowd.co.uk/home/stds/

Payment Services Directive (PDS2) and Strong Customer Authentication (SCA)

- PSD2 regulates payment services and payment service providers throughout the European Union (EU) and European Economic Area (EEA).[89]
- To comply with PSD2, payment transactions online require Strong Customer Authentication (SCA). This means that all transactions require at least two of the following:
  - Something that the customer knows (for example, a password or a pin)
  - Something that customers have (for example, a hardware token or a smartphone)
  - Something that the customer is (such as a fingerprint or a facial recognition scan).

The UK FinTech sector is being held back by difficulties involved in verifying the identities of new customers remotely. According to TechUK, "if the current status quo of inaction in terms of digital Identity persists [in the United Kingdom], this could lead to a 50 per cent increase in cases of identity fraud by 2021 and an additional associated cost of £2.5 billion by 2021 to the banking industry *alone*".[90] A reliable digital ID is crucial to the provision of financial services so that financial service providers (FSPs) can match that information against other sources to carry out customer due diligence (CDD).

Legal Identifiers and Corporate Digital IDs

Companies have a legal status equivalent to that of a person in many areas of common law. This allows them to enter contracts, be taxed, own property and seek redress in court.[91] As a result, businesses have the same need as citizens to assert and verify their identity on a daily basis, as part of the normal pursuit of their commercial activities.[92] Moreover, directors or employees often have to prove that they are authorised to act on behalf of the company to complete transactions.

Furthermore, businesses also have various different sets of data related to them. This could include their financial status and ownership structure, licences and regulated activities, as well as court records, regulatory sanctions and consumer complaints data. In terms of private data sources, a company could link third party providers to the government services it used, such as HMRC tax accounts, details on imports/exports, or public sector contracts. Making it easier for businesses to combine and share this information would prevent businesses from having to consistently resubmit the same information, particularly when applying for Government procurement contracts, something that is a particular drag on SMEs.

There already exist a number of different global standards to allow businesses to identify themselves. The legal framework for a company to register a digital identity and use it in the same way as a person already

90. TechUK, *The case for digital IDs*, February 2019, link

91. Companies House, *Guidance, Incorporation and names*, 23 December 2019, https://www.gov.uk/government/publications/incorporation-and-names/incorporation-and-names

92. The Future of Commerce, *"What is digital identity? Understand your customer in 4 steps"*, https://www.the-future-of-commerce.com/2019/09/30/what-is-digital-identity/

89. **Payment services (PSD 2) - Directive (EU) 2015/2366**, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en

exists in countries like Sweden and Estonia.[93] There are a number of private sector initiatives working to expand the established and globally predominant LEI system to facilitate a verified digital signature process.[94] Moreover, as part of the Companies House digital transformation strategy, it is now possible to submit the application to register a company online, as well as update company information and file other necessary documents.[95] Each company is issued an incorporation certificate with a unique company number, which is published in a searchable database.[96]

Global standards for Corporate Digital Identity

An increasingly global economy has created the necessity for standards and systems that allow cross-border trade and verification of foreign firms, especially in financial services. This is because companies have a need to assess the risk of commercial transactions, which includes verifying details provided by a commercial partner about their company[97]. International commercial contracts must also be agreed with legal certainty under a system that can be relied upon to settle disputes and that enables a company to enforce their legal rights and protections.

Legal Entity Identifier (LEI)

- Created and operated by the Global Legal Entity Identifier Foundation (GLEIF) the LEI is a unique, 20-digit identifier that indexes a company's information in a centralized, verified database.[98]
- LEI adoption by businesses has grown rapidly since its launch in 2013[99]

uPort Self Sovereign Certification Platform:

- This is a blockchain based system built on Ethereum as an extension to the LEI and in partnership with the GLEIF.[100] It allows directors and other registered persons associated with an LEI to add their credentials and identity to the LEI index, which is first verified by their issuing regulatory body.

The Government should explore the establishment of a Business Digital Identity programme. This would could help to improve companies' access to government business support measures and make it easier to bid for Government contracts. It would also support small those applying for grant funds and R&D Tax Credits. BEIS have already investigated creating such a scheme with consultants from KPMG, a prototype for which can be found on GitHub.[101]

Opening Up the Economy: Digital Vaccination Certificates & Contactless ID transactions

Digital IDs could be used to help tackle the COVID-19 (Coronavirus) Crisis. Digital ID has a number of potential applications when it comes to fighting the COVID-19 pandemic:

93. TrustCubes, 17 October 2018, https://www.trustcubes.com/sign-documents-using-the-strong-identities-you-already-have-today/
94. See box below
95. Companies House, *Our Transformation*, 23 April 2018, https://companies-house.blog.gov.uk/2018/04/23/companies-house-our-transformation/
96. Companies House, *Guidance, Incorporation and names*, 23 December 2019, https://www.gov.uk/government/publications/incorporation-and-names/incorporation-and-names
97. **WEF**, *Global Trade Identity can be the cornerstone of paperless trade*, 13 May 2019, https://www.weforum.org/agenda/2019/05/global-trade-identity-can-be-the-cornerstone-of-paperless-trade/
98. **GLEIF**, https://www.gleif.org/en/
99. **GLEIF**, Q&A, https://www.gleif.org/en/about-lei/questions-and-answers
100. **Uport**, https://www.uport.me/
101. ComputerWeekly, *It's time to party! Yet another government digital identity scheme is on the way*, 6 July 2020, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Its-time-to-party-Yet-another-government-digital-identity-scheme-is-on-the-way; GitHub, https://github.com/UKGovernmentBEIS/BEIS-Digital-Business-Identity/find/master

- **Vaccine certification**: If a safe and effective coronavirus is identified, digital vaccine certification could be included within a national COVID-19 vaccination strategy. The concept of demonstrating vaccination is not novel – the carte jaune indicating immunisation against yellow fever was first introduced by the WHO in the 1950s.[98] A possible coronavirus vaccine creates the opportunities to give the carte jaune concept a digital makeover, through linking an individual's vaccination to an existing verified digital ID. An app or secure identity wallet (such as those described above) could be used to bring together biometric data (for confirmation of identity) and the vaccination certificate (for confirmation of vaccination).[102] Such identity wallets could be stored on users' phones rather than on a central server to preserve their privacy. The UK Joint Committee on Vaccination and Immunisation has indicated that were a vaccine to be made available, it would recommend that frontline health and social care workers, and those at increased risk of serious disease and death, would be prioritised to receive the vaccine.[103] Once vaccination commenced at a population-scale, the digital certificates could be used to incentivise the population to be immunised, as verified digital IDs could be a prerequisite for admittance to a limited number of settings where the risk of infection is higher (such as a nightclub, for example). Although a vaccine has not yet been developed and the UK Government has not outlined its approach to vaccination, it should nonetheless commence scoping, consultation and feasibility studies regarding the infrastructure to support digital vaccination certification.
- **Remote authentication and contactless identity transactions:** Due to the outbreak of COVID-19, there is a significant risk that Coronavirus pathogens could be passed on through the handling of identity documents. Decentralised digital ID apps/wallets (such as those described in chapter 1) could allow people to prove their eligibility to purchase goods or services through their smartphones by scanning a unique QR code. This would allow businesses to complete identity checks whilst also reducing the risk of further transmission of the virus. Nonetheless, in order for this to be possible not only is it essential that the companies operating those apps can verify the user data to ensure that it is accurate, but the Government must also ensure that legislation is amended so as to ensure that companies do not have a legal duty to use physical identity document. For example, TechUK have rightly pointed out that the Licensing Act 2003 (Mandatory Licensing Conditions) (Amendment) Order 2014 prevents a digital identity from being used for proof of age for the purchase of alcohol.

102. Centre for Data Ethics and Innovation Blog, *Explainer: Immunity certificates*, https://cdei.blog.gov.uk/2020/06/15/cdei-explainer-immunity-certificates/

103. Joint Committee on Vaccination and Immunisation: Interim advice on priority groups for COVID-19 vaccination, 18 June 2020, https://www.gov.uk/government/publications/priority-groups-for-coronavirus-covid-19-vaccination-advice-from-the-jcvi/interim-advice-on-priority-groups-for-covid-19-vaccination

Recommendations

The UK Government must determine the role of the state in supporting innovation in, and the development of, the wider Digital ID 'ecosystem'. In the UK, the market for digital identity services is fragmented and complex to navigate. Unless action is taken, it is likely that market monopolies may be established in the future. The UK Government has an important role to play in the future of the digital ID market in the UK by:

- **Clarifying Liabilities and Setting Regulatory Standards:** Issues of liability will arise whenever a party suffers a financial loss as a result of a mistake made during the identity transaction process.[104] The lack of clarity as to who is liable when mistakes are made is hampering the UK digital ID market. As Tech UK points out, "there are differing schools of thought on liability models for digital identity" and, unless these divisions are sorted out, the market will not develop.[105]
- **Access to Public Sector Data Assets:** The Government also has access to large data assets that could be used to verify the identities of those trying to access services provided by the private sector. The Government needs to determine whether companies should be given access to such data assets to help them prevent fraud. Nonetheless, they must do so in such a way that preserves privacy. To do so the Government should expand the scope of the Document Checking Service (see below).
- **Encouraging Remote Authentication and Contactless Identity Transactions:** The UK Government should amend legislation (such as the Licensing Act 2003) that mandates private sector companies to check physical documents so as to remove barriers to the use of digital identities.
- **Prepare for digital vaccination certificates.** Once, and if, a vaccine is developed, evidence that a citizen has received the immunisation through the official UK programme could be linked to a verified digital ID, secured and stored in a decentralised way on a user's phone. Individuals could use their verified digital IDs to gain access different settings where the risk of infection is higher (such as a nightclub, for example) so as to ensure that the vulnerable are not exposed to the virus. The complexities associated with delivering such a scheme would be significant, including mitigating the risk of vaccine fraud. Therefore, scoping and feasibility assessment must commence now. Importantly, the certification process must be tied to vaccination rather than the presence of antibodies – given the well-known issues associated with immunity passports.

104. OIX, *The Vocabulary of Identity Systems LIability*, June 2014, https://openidentityexchange.org/wp-content/uploads/2014/06/White-Paper-The-Vocabulary-of-Identity-Systems-Liability.pdf

105. Tech UK, *The case for digital IDs*, February 2019 https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf

Digital ID in the UK Public Sector

Improving Access to Public Services

Digital identity is of particular importance to the public sector. Digitising public services not only improves their access and availability but can also lead to economic efficiencies. Nonetheless, unless people are able to prove that they are who they say they are online (to a high level of assurance) there will always be a bottleneck on the development of digital public services. More pertinently, fraudsters will thrive unless the Government develops reliable and accessible mechanisms to prove identity when accessing public services and supports the development of a fully functioning digital identity ecosystem in the private sector.[106]

The Government is at a crucial turning point when it comes to digital ID. Its main cross-departmental identity assurance platform, GOV.UK Verify, was supposed to be 'handed over' to the private sector in April 2020 and to cease receiving Government funding.[107] Instead, it was announced that GOV.UK Verify would receive an additional 18 months of funding due to COVID-19 and be prohibited from adding additional services to its roster.[108] There are rumours that GOV.UK Verify will be replaced by an 'Identity and Attributes Exchange', but unless lessons are learnt from the first attempt to establish an identity market in the UK, it is unlikely to be successful.[109]

It is divided into three sections. It will explore:

1. The context to digital ID in the UK public sector
2. Accessing Public Services online and the limitations to GOV.UK Verify
3. The Next Steps for Digital ID in the UK

The Government must preserve traditional identity checks. Although this chapter seeks to emphasise the benefits of digital identity and how it can improve access to public services, it is important to note that, even as progress is made when it comes to digital identity policy, traditional methods of identity checks should be preserved. There will always be certain individuals who either lack the skills or resources to create and use digital IDs and others who may feel uncomfortable about digital IDs. Any digital ID policy is likely to have greater public support if it is made clear

106. Policy Exchange, *Daylight Robbery*, 11 July 2020, https://policyexchange.org.uk/publication/daylight-robbery/
107. Civil Service World, *"Government to hand GOV.UK Verify over to private sector and cease funding"*, 10 October 2018, https://www.civilserviceworld.com/articles/news/government-hand-govuk-verify-over-private-sector-and-cease-funding
108. ComputerWeekly, *HM Treasury tells GDS: No further online services can use Gov.uk Verify*, 7 May 2019, https://www.computerweekly.com/news/252482828/HM-Treasury-tells-GDS-no-further-online-services-can-use-Govuk-Verify
109. ComputerWeekly, *Meet the Identity and Attributes Exchange – GDS's future for digital identity after Verify*, 9 June 2020, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Meet-the-Identity-and-Attributes-Exchange-GDSs-future-for-digital-identity-after-Verify

that digital IDs will not be mandatory and that it will always be possible to access public services that require identity checks in a traditional way by presenting identity documentation in person at a government office (for example). Although the same commitment should not necessarily apply to businesses or company directors (HMRC rightly has an ambition to become one of the most digitally advanced tax administrations in the world and its Making Tax Digital programme will require tax reporting to be entirely digital), preserving traditional methods of identity verification for public services are an important antidote to public concerns about digital identity.[110]

The context to digital ID in the UK

The UK's foundational difficulty

Many OECD nations, especially those in the EU, already have national digital identity schemes. Belgium (Itsme), Denmark (NemID), Finland (TUPAS), France (Alicem), Italy (SPID), Norway (BankID), The Netherlands (DigiD), Poland, Sweden (BankID) and Switzerland (SwissID) have introduced national digital identity programmes, many of which involve citizen biometrics.[111] These tend to be based on citizen registries in which all residents are provided with a national identity number or common identifier. These services (like those in Estonia) allow citizens not only to access services physically through an identity card but also digitally and remotely.[112] Although these services offer high user-control, for the most part they are founded upon a state-issued identity card.

e-ID and Mobile ID in Estonia

In Estonia every citizen has a state-issued identity card. This is accompanied by a digital ID, which allows citizens to identify themselves. This ID-card system also provides digital access to all of Estonia's secure e-services. It has two parts:

- **e-ID:** The chip on the card carries embedded files, and, using 384-bit ECC public key encryption, it can be used as definitive proof of ID in an electronic environment. It can be used for legal travel ID for Estonian citizens travelling within the EU, as a national health insurance card, as proof of identification when logging into bank accounts, for digital signature, for i-Voting, to check medical records, submit tax claims and to use e-Prescription services.
- **Mobile-ID:** allows people to use a mobile phone as a form of secure digital ID. Like the ID-card, it can be used to access secure e-services and digitally sign documents, but has the added advantage of not requiring a card reader. The system is based on a special mobile SIM card, which the customer must request from the mobile phone operator. Private keys are stored on the mobile SIM card along with a small application delivering the authentication and signature functions.

110. HMRC, *Overview of Making Tax Digital*, 21 July 2020, *https://www.gov.uk/government/publications/making-tax-digital/overview-of-making-tax-digital*
111. PUBLIC, *Towards a Common European Digital Identity*, 2 November 2019, https://www.public.io/towards-a-common-european-digital-identity/
112. E-Estonia, e-Identity, https://e-estonia.com/solutions/e-identity/id-card/

UK citizens do not have a universal common identifier upon which a digital ID programme might be based. Instead, UK citizens have many separate forms of identity documentation. These are issued by a range of bodies at different levels of Government, including the Home Office (via the Passport Office), HMRC, DWP, NHS, HMRC, DVLA and Local Authorities.[113] Furthermore, there is a long-standing political commitment in the UK not to introduce identity cards.[114] The UK's decision not to introduce biometric identity cards means that it lacks a universally held common identifier for all its citizens.[115] Common identifiers have been used as the backbone for digital identity services - across both the public and private sector - in many European countries.[116] This unique foundational difference has meant that businesses (and Government Departments) have had to create their own work-around solutions when it comes to digital identity.[117]

The Reasons for This Difference

Two views have defined Government policies towards identity for the past two decades. The Parliamentary Office of Science and Technology (POST) report "Electronic Government: Information Technologies and the Citizen" in February 1998 set out these two opposing views:

- **An official government-backed identity card:** "it is the responsibility of government to provide an official 'citizens card' once it expects people to use it to access and validate official transactions - just as it provides other documents such as passports and driving licences".[118]
- **The cultivation of a marketplace of identity providers:** "if there is a 'market' for 'identity' then it can be met by any number of private means and does not need a single official mechanism which could be portrayed by some as the equivalent of a national identification card".[119]

The UK's attempt to establish a centralised register of UK citizen attributes and to provide them with biometric identity cards was met with a public backlash. Due in part to the incoherence of different forms of identity and also in reaction to terrorist attacks of September 2001, the Government proposed an identity policy which culminated in the Identity Cards Act of 2006.[120] This Act aimed "to facilitate a secure and reliable record of registrable facts about individuals in the United Kingdom and to ensure a convenient method for individuals to prove registrable facts about themselves."[121] Organisations accredited by the Identity and Passport services were to be provided with digital certificates to allow them to verify information against the Identity Register via card readers.[122] Such a scheme could have been developed to allow people to access Government and other services online, as it has been done in many other countries.[123]

The UK Government has a long-term commitment not to introduce biometric identity cards. Due to political controversy, the Coalition

113. GOV.UK, *Proof of Identity Checklist*, 2014, https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist
114. Home Office, *Press Release, ID cards consigned to history, 22 December 2010* https://www.gov.uk/government/news/id-cards-consigned-to-history
115. BBC, Identity Cards Set to be scrapped, 12 May 2010, http://news.bbc.co.uk/1/hi/uk_politics/election_2010/8679072.stm
116. E-estonia, *e-identity*, https://e-estonia.com/solutions/e-identity/id-card/
117. Gemalto, *Top 5 digital ID trends shaping 2020 and beyond, Jan 2020*, https://www.gemalto.com/govt/identity/digital-identity-services/trends
118. Parliamentary Office of Science and Technology (POST) report "Electronic Government: Information Technologies and the Citizen" in February 1998 quoted in NTOUK, 'Online Identity' , accessed June 2020, https://ntouk.wordpress.com/e-government-and-digital-government-archives/online-identity/
119. Parliamentary Office of Science and Technology (POST) report "Electronic Government: Information Technologies and the Citizen" in rFebruary 1998 quoted in NTOUK, 'Online Identity' , accessed June 2020, https://ntouk.wordpress.com/e-government-and-digital-government-archives/online-identity/
120. BBC, *A question of identity*, 25 September 2001, http://news.bbc.co.uk/1/hi/uk/1562427.stm
121. GOV.UK, *The National Identity Register*, http://www.legislation.gov.uk/ukpga/2006/15/crossheading/registration/enacted/data.xht?view=snippet&wrap=true
122. Theyworkforyou, *Identity Cards, Home Department written question – answered on 7th March 2007*, https://www.theyworkforyou.com/wrans/?id=2007-03-07b.120388.h
123. Gemalto, *5 reasons for Electronic National ID Cards*, https://www.gemalto.com/govt/identity/5-reasons-electronic-national-id-card

Government of 2010 eschewed the introduction of a centralised identity database.[124] So long as the Government is committed to enabling a digital identity system fit for the UK's growing digital economy without the need for identity cards, it will have to take a different approach to countries like Estonia.[125] Nonetheless, Biometric Residence Permits are still issued to non-EEA nationals who apply to come to the UK for longer than 6 months, extend their visa for longer than 6 months or apply to settle in the UK.[126]

Biometric Residence Permit

- A Biometric Residence Permit is proof of a right to reside, work or study in the UK. A Biometric Residence Permit can also be used as a form of identity, for example to open a UK bank account.
- As Policy Exchange highlighted in *The Border Audit*, BRPs have been hugely successful at improving the UK's internal borders and in ensuring that BRP holders can prove their eligibility to access services provided by the public sector (such as healthcare) or by the private sector (for example, opening a bank account).[127]

Different Identity Management Systems

The UK Government has a number of different identity management systems. These are used by departments and agencies to verify the identities of citizens accessing their services. The two main ones are:

- **HMRC Government Gateway:** The pan-government Government Gateway Transformation Programme (GGTP) is an HMRC programme and is key to the government's digital transformation agenda. GGTP provides access to over 120 government services, provides credential management, hosts relevant databases and manages defined bulk data transfers of data between government and organisations. At its core, "Gateway" is a system for creating a user ID and password for use with Government services. Since its creation HMRC have added support for 2nd Factor Authentication. HMRC data is used to ask verification questions and to create an ID you need to submit your passport number.
- **GOV.UK Verify:** GOV.UK Verify is an eIDAS-compliant digital identity service that provides identity assurance for Government Departments.[128] GOV.UK Verify allows citizens to prove their identities online when accessing Government services. It operates without a central government database of citizen attributes and works with certified companies, known as identity providers (IDPs), to prove users' identities. In order to create a Verify account you have to provide some personal information which is then checked against a variety of different records. Once these have been checked, you can use Verify to access Government services online such as the receipt of benefits or to pay tax bills. GOV.UK

124. Home Office, *Press release, National identity register destroyed as government consigns ID card scheme to history,* https://www.gov.uk/government/news/national-identity-register-destroyed-as-government-consigns-id-card-scheme-to-history

125. NAO, *Identity Assurance Programme*, 2014, https://www.nao.org.uk/wp-content/uploads/2014/12/Identity-Assurance-Programme1.pdf;

GDS, Why GOV.UK Verify Matters, 23 September 2015, https://gds.blog.gov.uk/2015/09/23/why-gov-uk-verify-matters/;

The Register, UK.gov drives ever further into Nocluesville, crowdsources how to solve digital identity, https://www.theregister.co.uk/2019/07/19/gov_asks_public_how_to_solve_digital_identity/

126. GOV.UK, *Biometric Residence Permits*, https://www.gov.uk/biometric-residence-permits

128. GOV.UK, *Privacy Notice*, 22 October 2019, https://www.signin.service.gov.uk/privacy-notice https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2018/09/11/GOV.UK+Verify+eID+scheme+pre-notified+under+eIDAS

127. Policy Exchange, *The Border Audit*, 2018, https://policyexchange.org.uk/wp-content/uploads/2018/07/The-Border-Audit.pdf

Verify was designed with the intention of preserving user privacy. **There are other identity management systems in the public sector.** Many Local Authorities have developed their own sign-in platforms. Furthermore, every UK citizen has an NHS number and patients can access their health records via NHS Login and the Law Society, the Council for Licensed Conveyancers (CLC) and the Chartered Institute for Legal Executives (CILEx) have recently announced that they will be collaborating together to examine using digital identity in conveyancing and to support property transactions.[129]

NHS Login

- **NHS numbers:** An NHS Number is a 10-digit number and is unique to every NHS patient. NHS numbers are used by healthcare staff and service providers to identify patients correctly and match their details to health records.
- **NHS login:** This is a service that has been created by the NHS for patients and the public. It provides a re-usable way for patients to access multiple digital health and social care services with a single login, which includes authentication for returning users. NHS login can be used by the public to securely access their health and care information wherever they see the NHS login button. People can use an NHS login to prove who they are safely and securely and, in most cases, without the need to visit their GP.

The Department of Work and Pensions is also designing its own alternative to Verify.[130] Due to the problems that claimants experienced when trying to prove their identities to access Universal Credit, the Department of Work and Pensions was forced to develop its own digital ID solution. It is called *Confirm Your Identity* which helps Universal Credit claimants prove their identity online during the application process.[131] At the start of the Coronavirus (COVID-19) Crisis, the Department of Work and Pensions had to connect HMRC Government Gateway to support Verify which was unable to cope with the number of people who needed to prove their identity to access universal credit.[132]

HMRC's Government Gateway Service was supposed to be replaced by GOV.UK Verify. Nonetheless, GOV.UK Verify did not develop the capacity to delegate authority for others to act as intermediaries, making it extremely difficult for it to be used for the purposes of paying tax.[134] This meant, for example, that accountants couldn't file their clients' tax returns. At present, the two services now run side-by-side on many platforms most notably on HMRC's personal tax account.[135]The majority of people trying to pay their tax use HMRC Government Gateway to complete a self-assessment.[136]

129. HM Land and Registry, *Facing up to the digital identity challenge*, 29 May 2020, https://hmlandregistry.blog.gov.uk/2020/05/29/facing-up-to-the-digital-identity-challenge/
130. The Register, *DWP building a separate ID tool as Verify can't cut it, whisper sources*, 14 Jan 2016, https://www.theregister.co.uk/2016/01/14/dwp_indicates_its_building_a_separate_online_id_tool/
131. Computerweekly, *Why Gov.uk Verify faces a critical few months - again, 5 August 2019*, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/Why-Gov-uk-Verify-faces-a-critical-few-months-again
132. Computer Weekly, *DWP Turns to Government Gateway to Support Universal Credit Claimants*, https://www.computerweekly.com/news/252481687/DWP-turns-to-Government-Gateway-to-support-Universal-Credit-claims?_
134. Computer Weekly, *HMRC ID vs Gov.uk Verify – what's the difference, and why it matters*, 15 February 207, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/HMRC-ID-vs-Govuk-Verify-whats-the-difference-and-why-it-matters
135. GDS, *GOV.UK Verify's Role in HMRC's Highest Self-Assesment Peak*, July 2019 https://gds.blog.gov.uk/2019/07/30/gov-uk-verifys-role-in-hmrcs-highest-self-assessment-peak/
136. GDS, *GOV.UK Verify's Role in HMRC's Highest Self-Assesment Peak*, July 2019 https://gds.blog.gov.uk/2019/07/30/gov-uk-verifys-role-in-hmrcs-highest-self-assessment-peak/

GOV.UK Verify: How does it work and why was it developed?

The Coalition Government attempted to revitalise the delivery of public services by reinventing Government 'as a platform'. The idea of 'Government as a platform' was to create a single, digital channel through which Government activities can be operated. This would improve the delivery and efficiency of public services, reducing overlap between different departments and enhancing the set of digital tools and infrastructure available to the Government.[137] On the 18th May 2011, Francis Maude MP (Minister for the Cabinet Office and Paymaster General) announced to Parliament that:

> *"the Government agreed on 14 March 2011 to the development of a consistent, customer-centric approach to digital identity assurance across all public services. This will allow service users to log on safely to digital public services in a way that ensures personal privacy, reduces fraud and facilitates the move to online public services."*[138]

GDS, Digital by Default and Government as a Platform

- **The Government Digital Service (GDS) was established as a Unit of the Cabinet Office in 2011.** This followed Martha Lane Fox's *Directgov 2010 and beyond: revolution not evolution.*[139] It aimed to enable the implementation of a "digital by default" approach to public services and helped the UK reach the top spot on the United Nations e-government survey in 2016.[140] Since 2010, it has combined nearly 2,000 government websites into a single site GOV.UK.[141]
- **The introduction of the GOV.UK website provided the initial step towards this ideal.** Other projects undertaken include:
  - **GOV.UK Notify** automates email and text message reminders
  - **GOV.UK Pay** handles small financial transactions and fines
  - **GOV.UK Verify** provides identity assurance for Government Departments
- **Notify, Verify and Pay has been adopted by numerous government departments.** Over half of Government Departments use GOV.UK Pay, and all but two use GOV.UK Notify.[142] As Policy Exchange has frequently pointed out, moving towards common platforms was - and remains - a challenge for individual Government Departments who want to avoid a loss of functionality by moving away from systems in which they have invested significant resources and which may be perfectly tailored to their needs.[143]

The design of GOV.UK Verify was guided by the Government's decision to repeal the Identity Cards Act on 21 January 2011. To avoid establishing a central Government database or citizen registry, GOV.UK Verify was designed with a "federated" architecture in which the task of verifying identities was outsourced to a set of private companies, each of which had to go through rigorous checks to make sure they could be trusted to keep identity data secure.[144] Crucially, the use of private companies meant that the Government could receive identity assurance "without the need for ID cards".[145]

137. Cabinet Office, Government Digital Strategy, 2013, https://www.gov.uk/government/publications/government-digital-strategy/government-digital-strategy
138. Hansard, *18th May 2011*, https://hansard.parliament.uk/Commons/2011-05-18/debates/11051863000014/IdentityAssurance
144. GDS, *How we introduce GOV.UK Verify*, 17 August 2016, https://identityassurance.blog.gov.uk/2016/08/17/how-we-introduce-gov-uk-verify/
145. DCMS and Cabinet Office, *Digital Identity Call for Evidence*, July 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf
139. GOV.UK, *Independent Report*, Directgov 2010 and beyond: revolution not evolution, 2010, https://www.gov.uk/government/publications/directgov-2010-and-beyond-revolution-not-evolution-a-report-by-martha-lane-fox
140. UN, E-Government Survey, 2016, https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2016
141. GDS, *Transforming GOV.UK: the future of digital public services* https://gds.blog.gov.uk/2019/11/05/transforming-gov-uk-the-future-of-digital-public-services/
142. Institute for Government, *Whitehall Monitor: Dgital, 2020*, https://www.institute-forgovernment.org.uk/publication/whitehall-monitor-2020/digital
143. Policy Exchange, *The Smart State, 2018*, https://policyexchange.org.uk/wp-content/uploads/2018/05/The-Smart-State-1.pdf; Policy Exchange, *Whitehall reimagined, December 2019*, https://policyexchange.org.uk/publication/whitehall-reimagined/, Policy Exchange, *How To Transform the Government's Digital Leadership*, https://policyexchange.org.uk/how-to-transform-the-governments-digital-leadership/

Federated Identity Schemes
• Digital Identity schemes with a federated architecture allow accredited private companies to verify the identities of individuals to a set of agreed standards. Once verified, citizens can access various government services and portals.[146]
• Identity providers use a variety of data sources to validate users. These data sources can be held by both the private sector (for example, financial transactions or credit histories) or the public sector (e.g. government records).[147]

It is important to understand precisely what is meant by 'GOV.UK Verify'. 'GOV.UK Verify' refers not only to the development of the Verify platform (i.e. the physical IT system), but also an online identity assurance framework that was supposed to establish common digital identity standards across both the public and private sectors.[148] It also established a commercial framework to determine how much Government departments should pay for identity assurance from third parties.[149] It provides verification checks and ensures that IDPs cannot see which services users are accessing, and similarly ensures that Government departments don't see information about their users: only that they are eligible.[150] At its onset, the Privacy and Consumer Advisory Group (PCAG) developed 9 principles to govern its use:

Identity Assurance Principles	Summary of the Identity Assurance Principles
The User Control Principle	Identity assurance activities can only take place if I consent or approve them.
The Transparency Principle	Identity assurance can only take place in ways I understand and when I am fully informed.
The Multiplicity Principle	I can use and choose as many different identifiers or identity providers as I want to.
The Data Minimisation Principle	My request or transaction only uses the minimum data that is necessary to meet my needs.
The Data Quality Principle	I choose when to update my records.
The Service-User Access and Portability Principle	I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want.
The Governance/ Certification Principle	I can trust the Scheme because all the participants have to be accredited.

148. See chapter 1

149. Computer Weekly, *How to accelerate digital identity in the UK*, https://www.computerweekly.com/opinion/How-to-accelerate-digital-identity-in-the-UK

150. LSE Research Online, *Trusted digital identity provision: GOV.UK Verify's federated approach*, 2018, http://eprints.lse.ac.uk/90577/1/Whitley_Trusted%20digital%20ID_2018.pdf

146. **LSE Research Online**, *Trusted digital identity provision: GOV.UK Verify's federated approach*, **2018**, http://eprints.lse.ac.uk/90577/1/Whitley_Trusted%20digital%20ID_2018.pdf

147. **LSE Research Online**, *Trusted digital identity provision: GOV.UK Verify's federated approach*, **2018**, http://eprints.lse.ac.uk/90577/1/Whitley_Trusted%20digital%20ID_2018.pdf

The Problem Resolution Principle	If there is a problem I know there is an independent arbiter who can find a solution.
The Exceptional Circumstances Principle	Any exception has to be approved by Parliament and is subject to independent scrutiny.

GOV.UK Verify was intended to kickstart the digital ID market for digital identity in the UK. In addition to creating a common identity assurance platform for the Government, it also aimed to leverage the Government's need for identity assurance to create a private sector market for identity assurance based on common standards.[151] Once users had created a verified identity through the Government, it would be possible for these users to use their "verify'd" identities to access services for private sector identity transactions. GDS expected the programme to cost £212 million and generate benefits of £873 million over four years from 2016-17 to 2019-20.[152]

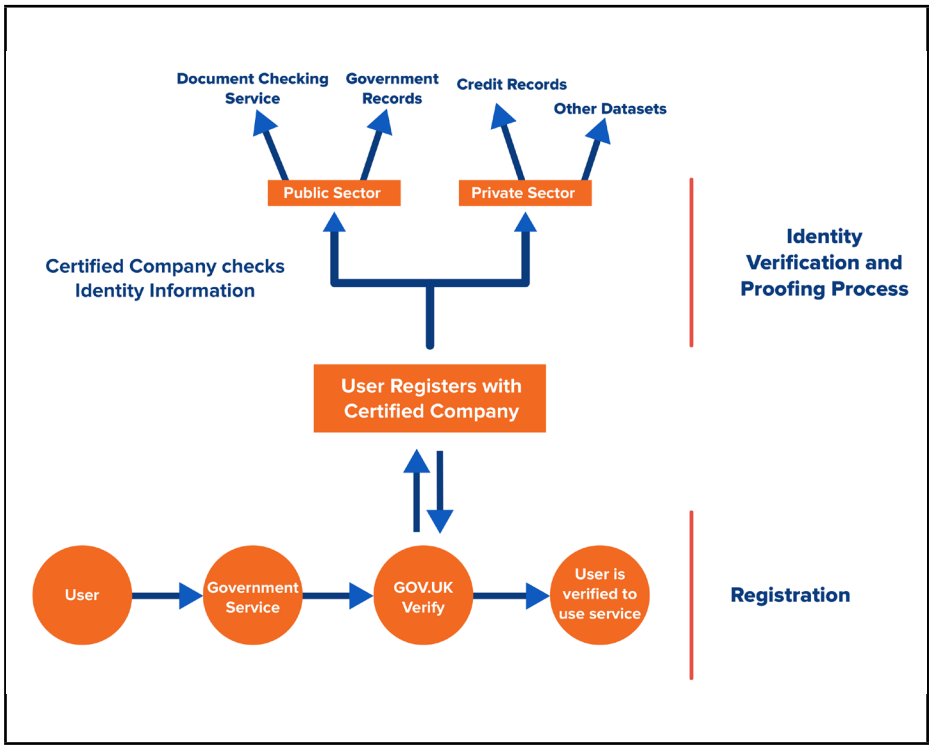
How does GOV.UK Verify work?

GOV.UK Verify is a risk-based service, based on trust. It allows the verification process to be carried out by private sector Identity Providers, or IDPs. These are companies that meet the standards set by the Government to verify and authenticate the identities of users. These IDPs are paid by Government departments to do so. This means that multiple identity providers can compete to attract customers and encourages innovation in both verification and authentication activities.

To create an account, each user goes through a four step-process. Once users have created an account, they can reuse it to access services provided by other departments that are connected to the GOV.UK Verify Hub. These four initial steps are:

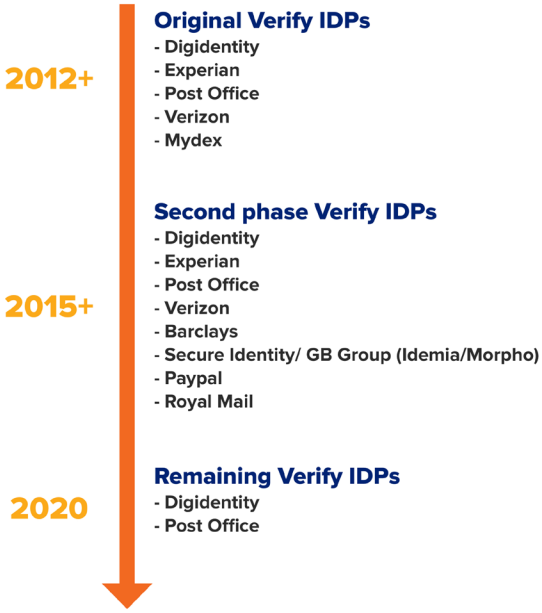
1. **GOV.UK:** A user wishing to verify their identity online to access Government services visits the GOV.UK website.
2. **Choosing an Identity Provider:** Instead of sending all of their information to the Government Department, they choose an 'identity provider' to vouch for them. Originally, there were seven companies that provided this service but several have dropped out.
3. **Authentication:** The chosen company checks their personal details against records held by mobile phone provider, credit agencies, HM Passport Office or the DVLA. Verify has its own Document Checking Service (DCS), which allows providers to query passport and driving license data. This allows them to make sure that the information provided is correct.
4. **Verification:** having checked that your identity documents are accurate, authentic and valid, the external identity provider simply confirms to the Government Department whether or not you have met the criteria. It does this without transferring any sensitive information.

151. Public Technology, *Interview with Oliver Dowden*, https://www.publictechnology.net/articles/features/interview-oliver-dowden-verify-spending-controls-and-how-'gds-moving-new-spaces'
152. National Audit Office, *Investigation into Verify*, March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf



Many of the certified companies acting as identity providers have dropped out. At present, there are only two companies that act as identity providers through the GOV.UK Verify framework. These are the Post Office and Digidentity, although both run off the same back-end identity engine. In May 2020, it was confirmed that Barclays, Experian, and SecureIdentity had withdrawn, effectively forcing those users to re-create an account with another provider.[153] Although the GDS has run a pilot in which non-public sector companies can use the document checking service, Verify has not been used to provide identity assurance for the private sector.

153. ComputerWeekly, *DWP takes Centre Stage in Future of GOV.UK Verify*, 11 May 2020, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/DWP-takes-centre-stage-in-future-of-Govuk-Verify?_ga=2.34113895.758846749.1591016742-466382040.1591015386



The Document Checking Service and Document Checking Service Pilot

- The Document Checking Service checks passport details against the HM Passport Office (HMPO) database. It provides a simple 'yes' or 'no' response to say whether a passport is valid without giving direct access to government-held data.
- It is a huge economic asset to the Government due to the fact that it could transform identity assurance in the private sector (particularly in the financial service and FinTech Sectors) by allowing private sector organisations to use it to check the identities of their customers.
- The Document Checking Service Pilot allows the non-public sector organisations participating to pay to access the service to find out if British passports are valid.
- Under the terms of the pilot, it costs 50p per check in the document checking service. In addition to this, participants also had to pay a connection fee, tiered by the volume of checks that they wanted to do.[154]

The Limitations to the Government's Current Approach

GOV.UK Verify has come under considerable criticism. The platform missed its original 2012 live implementation date by nearly four years and by the time of its live implementation was working with just 12 services (well short of the 100 originally predicated), many of which also offered alternatives to Verify.[155] In March 2019, the National Audit Office also found that "it is difficult to conclude that successive decisions to continue with Verify have been sufficiently justified." Similarly, the Infrastructure and Projects Authority (IPA) marked Verify as "Red".[156] This means that

155. NAO, *Digital Transformation in Government*, March 2017, https://www.nao.org.uk/report/digital-transformation-in-government/;

Computer Weekly, *GOV.UK Verify and Identity Assurance: Time For A Rethink*, 2017, https://www.computerweekly.com/opinion/Govuk-Verify-and-identity-assurance-its-time-for-a-rethink

156. Infrastructure and Projects Authority, GOV.UK Verify: Project Assessment Review (PAR), February 2017

154. GOV.UK, *Guidance, The Document Checking Service pilot scheme*, 22 February 2020, https://www.gov.uk/guidance/apply-for-the-document-checking-service-pilot-scheme

the:

> *"successful delivery of the project appears to be unachievable. There are major issues with project definition, schedule, budget, quality and/or benefits delivery, which at this stage do not appear to be manageable or resolvable. The project may need re-scoping and/or its overall viability reassessed."*[157]

Likewise, the Public Accounts Committee found that "GDS has failed to meet any of its original performance targets for Verify and vastly overestimated the benefits it could achieve" and that "people using Verify have been badly served by an onerous system that is not fit for purpose."[158] Unless these limitations are recognised, it is unlikely that future attempts to provide identity assurance for the public sector will be successful.

The Limitations of GOV.UK Verify

GOV.UK Verify has missed its targets. It has struggled in a number of key areas:

- **There have been poor levels of uptake.** It was expected that there would be 25 million users by 2020.[159] There were as of March 2020 (before the Coronavirus outbreak), only 5.8 million users.[160] This has meant that the identity providers who opted into the scheme made investments on the basis of the fact that they felt that there would be a user base over four times the size that it is currently.
- **GOV.UK Verify was not adopted across Whitehall.** The project aimed to have 46 Government services accessible by March 2018. At present, only 22 Government services use it.[161]
- **The Verification Success Rate is too low.** The GDS aimed to have a verification success rate (proportion of people who successfully sign up in a single attempt) of 90%.[162] Before the Coronavirus Crisis, it had a verification success rate of 44%.[163] The authors of this report are sceptical of the utility of the verification success rate as a useful performance metric. GOV.UK Verify's primary purpose was to prevent fraud and it is highly likely that more than 10% of those trying to access services were fraudulent. Nonetheless, it is not inconceivable that some people who need to access Government services have been denied access simply because private companies cannot verify their identity, something that is particularly important in the case of "thin-file" individuals.[164]
- **GOV.UK Verify has not generated the benefits it expected.** It was expected to generate benefits of £873 million over four years from 2016-17 to 2019-20. According to the National Audit Office, the actual number was only £217 million (75% lower).[165] Moreover, as the Commons Public Accounts Committee has pointed out, "an unknown amount of costs have been shunted onto other government departments, such as the costs of reconfiguring their systems to use Verify and additional manual processing costs for

157. Infrastructure and Projects Authority, *Annual Report on Major Projects 2018-19*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817654/IPA_AR_MajorProjects2018-19_web.pdf
158. House of Commons Committee of Public Accounts, *Accessing public services through the Government's Verify digital system*, 8 May 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/1748.pdf
159. DCMS, *Digital government - maintaining the UK government as a world leader in serving its citizens online, 1 March 2017*, https://www.gov.uk/government/publications/uk-digital-strategy/6-digital-government-maintaining-the-uk-government-as-a-world-leader-in-serving-its-citizens-online, GOV.UK, *Dashboard GOV.UK Verify*, https://www.gov.uk/performance/govuk-verify
160. GOV.UK, *Dashboard GOV.UK Verify*, https://www.gov.uk/performance/govuk-verify
161. GOV.UK, *Dashboard GOV.UK Verify*, https://www.gov.uk/performance/govuk-verify
162. National Audit Office, *Investigation into Verify*, March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf;

    Go, *GOV.UK Verify: Understanding Who can be Verified*, January 2015, https://gds.blog.gov.uk/2016/01/25/gov-uk-verify-understanding-who-can-be-verified/
163. GOV.UK, *Dashboard GOV.UK Verify*, https://www.gov.uk/performance/govuk-verify
164. This is particularly important given that DWP is GOV.UK Verify's biggest customer. Those on Universal Credit have a higher chance of being "thin-file" individuals than wealthier peers.
165. National Audit Office, *Investigation into Verify*, March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf

people unable to use Verify."[166]

- **GOV.UK Verify remains subsidised.** This means that Departments do not pay their full usage costs for verifying the identities of those with whom they interact, meaning that the GDS subsidises GOV.UK Verify.[167] It was expected to be self-funding by the end of March 2018 when the Government was supposed to cease funding the programme centrally.[168] This was then extended for a further 18 months and then again in April 2020 due to the COVID-19 crisis.[169]
- **Identity Providers have dropped out.** As noted earlier, Experian, Barclays and Secure Identity notified GDS of their intention to pull out before May 2020.[170] This meant that everybody who created an account with one of these three certified companies would be forced to make a new Verify account.

Why GOV.UK Verify struggled

GOV.UK has struggled for a number of reasons:

- **Adoption by other Government Departments was not agreed before the project started.** As the NAO pointed out, "GDS and the Cabinet Office did not mandate the use of Verify at an early stage. Departments were able to continue using other identity verification systems."[171] This, in turn, meant that those in charge of the delivery of GOV.UK Verify (and the viability of the project, given the need of identity providers to justify their investment) were reliant upon departments who had not committed to the programme. It also meant that GOV.UK Verify had a small number of 'use cases', giving users a limited incentive to sign up.
- **GOV.UK Verify's levels of assurance were too rigid.** As one expert has put it "prescribing rigid levels of assurance (LOA) has hindered the uptake of digital identity, as risk-averse service providers have often opted for the highest possible LOA, which often introduces unnecessary friction for the user."[172] It might have been better to start at a very low level of assurance and to build up identity profiles over time.[173] Moreover, it has been suggested to the authors that there was an unnecessarily steep "cliff-edge" between LOA1 and LOA2. Creating more refined criteria would reduce user friction. Nonetheless, whilst this may be true, many of the transactions that GOV.UK Verify completed were fraud sensitive one-off transactions. Lower standards might have led to unacceptable levels of public sector fraud.
- **The Government missed opportunities to "onboard" people to Verify.** For example, since Britain voted to leave the European Union in 2016, many EU nationals have had to apply through the EU Settlement Scheme for settled and pre-settled status. This would have been a good opportunity to 'on-board' around 2.3 million EU citizens.[174]
- **The metrics used to assess the project were set incorrectly.**

166. https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/1748.pdf
167. National Audit Office, *Investigation into Verify*, March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf
168. Cabinet Office and GDS, *Government Transformation Strategy: role of the Government Digital Service*, 9 February 2017 https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-role-of-the-government-digital-service
169. See Above
170. *ComputerWeekly*, August 2019, link
171. National Audit Office, *Investigation into Verify*, March 2019, https://www.nao.org.uk/wp-content/uploads/2019/03/Investigation-into-verify-Summary.pdf
172. Computer Weekly, *How to accelerate digital identity in the UK*, https://www.computerweekly.com/opinion/How-to-accelerate-digital-identity-in-the-UK
173. Computer Weekly, *How to accelerate digital identity in the UK*, https://www.computerweekly.com/opinion/How-to-accelerate-digital-identity-in-the-UK
174. Home Office, *Rebuttal Media Articles on the EU Settlement Scheme*, August 2019, https://homeofficemedia.blog.gov.uk/2019/08/30/rebuttal-media-articles-on-the-eu-settlement-scheme/

Specifically, the "Verification Success Rate" is a poor metric to measure success**.** The verification success rate is determined by the proportion of people who sign up in a single attempt. Nonetheless, if the primary function of an identity verification platform is to prevent fraud from taking place, then there is no guarantee that 90% of the applications are genuine. If the platform successfully weeded out fraudulent identity assertions, or people did not proceed because they realised that they would not be able to pass through the tests, then a low success rate would be considered a success. Moreover, a poor verification success rate is not exclusive to GOV.UK Verify. Nearly 40% of banking applications are abandoned prior to completion.[175]

- **It was (arguably) not in the economic interests of identity providers to improve the pass-through rates.** To develop a low-friction onboarding experience, companies have to spend significant sums of money to constantly refine the process. Arguably, the economic incentive for the identity providers to invest time and resources in developing their user experience was not strong enough.
- **Verify operated according to a 'closed commercial framework'.** This meant that only a small number of companies were allowed to participate and act as 'certified companies' or 'identity providers'. Instead, it should have operated according to an open commercial framework. Under an open commercial framework, any company that met the standards and criteria for identity verification checks would have been able to act as a certified company and sell identification checks and services to the Government. There are a number of major limitations to this 'closed commercial framework':
  - **First, it meant that coverage was poor.** There are many people who do not have an account with one of the certified companies, meaning that they have to create one in order to register with Verify. This makes it more difficult for customers to sign up to GOV.UK Verify.
  - **Second, it hampered competition.** Since only a handful of companies are able to provide identities assurance to the Government, then there was no incentive for others to adopt common standards for identity assurance.
- **Should private companies determine access to public services?** As one critic of Verify put it: "how can it be right that the private sector was allowed to become the exclusive gatekeeper for deciding whether or not citizens can access online public services?"[176]
- **Poor decision making and oversight.** To quote the Public Accounts Select from its report *Accessing public services through the Government's Verify digital system*, its "witnesses did not take seriously enough their responsibilities to explain and account for why the programme failed to meet its original goal of providing a single

175. Signicat, What is an Electronic Identity, 18 February 2020, https://www.signicat.com/resources/what-is-an-electronic-identity?utm_campaign=TOFU%20%2F%2F%20What%20is%20an%20eID%20blog%20series%20%2F%2F%20Q12020&utm_source=twitter&utm_medium=paidsocial

176. Computer Weekly, Editor's Blog, 6 March 2019, https://www.computerweekly.com/blog/Computer-Weekly-Editors-Blog/NAO-hammers-another-nail-into-Gov-uk-Verify

identity assurance service across government. They chose instead to emphasise the work currently being done to develop a wider market for identity verification services. It is simply not good enough to rewrite the programme's aims after the event to try to explain away underperformance."[177]

The Next Steps in Digital ID

Recent Developments

Following a consultation, the Government announced the establishment of Digital Identity Strategy Board in September 2020. The Board has outlined 6 principles for digital ID going forward, similar to the PCAG guidance from 2014.[178] The government also updated two notable documents: Good Practice Guide 44 (using authenticators to protect an online service) and Good Practice Guide 45(how to prove someone's identity).[179]

The development of GOV.UK Accounts was also announced in September 2020.[180] A single sign-on service for GOV.UK, it will allow customers to "proactively offer information and services to users based on their needs and what they've told us about themselves, reduce friction for users so that they don't have to give different parts of government the same information multiple times [and] link together services to make user journeys simpler".[181] GOV.UK Accounts will not be equivalent to a digital ID since it does not appear to be based on verified user attributes. Indeed, the Cabinet Office have emphasised that their intention is not "to create an 'uber CRM' for the Government".[182] Nonetheless, over time, the system could *potentially* develop if users had the opportunity (using the document checking service) to increase the level of assurance in their GOV.UK Account.

177. House of Commons Committee of Public Accounts, *Accessing public services through the Government's Verify digital system*, 8 May 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/1748.pdf

178. Cabinet Office, Department for Culture, Media and Sport, *Digital ID: Call for Evidence Response*, 8 September 2020, https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response

179. Cabinet Office, DCMS, *Using authenticators to protect an online service*, https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services;

Cabinet Office, DCMS, *How to Prove Someone's Identity*, https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

180. Government Digital Service, *Introducing GOV.UK Accounts, 22 September 2020, https://gds.blog.gov.uk/2020/09/22/introducing-gov-uk-accounts/*

181. Government Digital Service, *Introducing GOV.UK Accounts, 22 September 2020, https://gds.blog.gov.uk/2020/09/22/introducing-gov-uk-accounts/*

182. Government Digital Service, *Introducing GOV.UK Accounts, 22 September 2020, https://gds.blog.gov.uk/2020/09/22/introducing-gov-uk-accounts/*

The Digital Identity Strategy Board's six principles

- **Privacy:** When personal data is accessed, people will have confidence that there are measures in place to ensure their confidentiality and privacy; for instance, a supermarket checking a shopper's age, a lawyer overseeing the sale of a house, or someone applying to take out a loan.
- **Transparency:** When an individual's identity data is accessed when using digital identity products, they must be able to understand by who, why and when; for example, being able to see how your bank uses your data through digital identity solutions.
- **Inclusivity**: People who want or need a digital identity should be able to obtain one; for example, not having documentation such as a passport or driving licence should not be a barrier to having a digital identity.
- **Interoperability:** Setting technical and operating standards for use across the UK's economy to enable international and domestic interoperability.
- **Proportionality:** User needs and other considerations, such as privacy and security, will be balanced so that digital identity can be used with confidence across the economy.
- **Good governance:** Digital identity standards will be linked to government policy and law. Any future regulation will be clear, coherent and align with the government's wider strategic approach to digital regulation. For example, firms verifying someone's identity will need to comply with laws around how they access and store data.

Improving Identity Proofing and Verification

The Government should use its National Data Strategy to identify public sector data assets that could support the identity proofing and verification processes. To verify a person's identity, companies acting as identity providers need to refer to a combination of official and commercially available data sources. This can happen either by validating documents through the Document Checking Service or drawing upon data from Credit Reference Agency (CRA) files.[183] Some 'thin-file users' may struggle to access services because of their weak digital footprints. The difficulty that those who were not on credit check databases experienced when trying to use the government's online coronavirus test and trace system to get a home test is the best example of this.[184] Likewise, a new release from prison transitioning to Universal Credit will need proof of their identity to make a claim. Despite the fact that prisoners have been directly with the state for the entirety of their sentences, many struggle to make this transition due to a lack of identity documents.[185] The more Government data that is available to verify identities, the less likely it is that there will be "thin file" individuals and the more inclusive the identity service.

183. See pp. 26-7

184. HJS, *Revealed: online covid tests refused to those not on credit check databases*, 8 June 2020, https://www.hsj.co.uk/coronavirus/revealed-online-covid-tests-refused-to-those-not-on-credit-check-database/7027794.article?adredir=1

185. Department of Work and Pensions, *Universal Credit and prison leavers*, 4 May 2018, https://ntouk.wordpress.com/2019/12/23/the-elusive-pursuit-of-outsourced-digital-identity/

Data sharing across Government should be a key priority. According to the National Audit Office, there are three issues hampering the use of data across Government:

- Data is not always seen as a priority;
- The quality of data is not well understood;
- There is a culture of tolerating and working around poor quality data.[186]

Although access to cross-governmental data is important for a number of activities, the national data strategy should be used as an opportunity identify identity proofing and verification as a particular priority. The Government's plan to produce a National Data Strategy was first announced in June 2018. The strategy's aim is to "drive the collective vision that will support the UK to build a world-leading data economy".[187] The National Data strategy has 5 missions. Mission 1 (unlocking the value of data across the economy) and mission 3 (transforming government's use of data to drive efficiency and improve public services) are of particular relevance to digital identity.

A digital identity strategy

The Government should also launch a separate digital identity strategy with a ten-year roadmap for digital identity. Such a strategy should emphasise the importance of the following principles to digital ID and public sector identity assurance:

- **High levels of user privacy and control:** Any Digital ID strategy should aim to give citizens the tools to control their own data and to preserve their privacy.
- **The role of common standards in increasing the use cases for digital IDs across both the public and private sector.** At present, GOV.UK Verify only has a small number of 'use cases', giving users a limited incentive to sign up. The more services that a user is able to access with a digital ID, the more likely they are to create and use one.
- **Finding the right balance between establishing high levels of assurance and making it easy to onboard users.** Forcing people to create a digital ID to a high level of identity assurance is necessarily time consuming and can discourage people from completing the necessary checks.[188] Finding a balance between ease of access and the high levels of assurance that are often required to access services is a key challenge for both the Government and private sector companies.

186. National Audit Office, *Challenges in Using Data Across Government*, June 2019, https://www.nao.org.uk/wp-content/uploads/2019/06/Challenges-in-using-data-across-government.pdf

187. DCMS, *National Data Strategy*, September 2020, https://www.gov.uk/guidance/national-data-strategy

188. Computer Weekly, *How to accelerate digital identity in the UK*, https://www.computerweekly.com/opinion/How-to-accelerate-digital-identity-in-the-UK

Settling on a reliable digital ID model

The Government must establish reliable models for public sector ID assurance. The UK Government has a number of different options when it comes to the future of digital ID. Legal frameworks are needed to allow the state to benefit from its central position as a trusted intermediate that can facilitate identity exchange. As the Open Identity Exchange remarked, the National Audit Office report into GOV.UK Verify "fails to account for the cost of doing nothing".[189]

The different options open to the Government include:

- **Encouraging departments and agencies to develop their own tailored ID solutions:** Such a policy decision would ensure that every identity solution would be tailored to the service for which it is designed to provide access. This may be worthwhile for the small number of high-value identity transactions which are unique and would create a suite of different identity solutions across Whitehall. Nonetheless, it may be difficult to create such solutions without the use of biometrics as is done in the private sector (raising civil liberties concerns). It could also result in departments duplicating processes, thereby increasing overall costs to the government, and it would make it more difficult for users who would have to manage multiple government accounts and digital identities.
- **Using the DWP *Confirm Your Identity* service and HMRC Gateway as the main identity solutions across Whitehall.** HMRC Gateway already provides access to a large number of Government services and when DWP's *Confirm Your Identity* service has been launched fully, it could fulfil a similar function, particularly if common identity standards are adopted across Government. Likewise, GOV.UK Accounts (still in protype form) could be developed over time into a reliable identity solution across Whitehall, particularly if it was supported by the Document Checking Service. Nonetheless, since these systems were designed to support specific transactions, they may well be unable to support some services, particularly if such transactions require high levels of identity assurance. Likewise, there are also likely to be concerns about civil liberties if these systems develop to support the use of biometrics. Furthermore, it may also be difficult to ensure that there is a frictionless user experience if such systems are unable to draw upon wide ranges of data (from both the public and private sectors) during the identity proofing and verification stages of an identity transaction.[190]
- **Continue to use accredited third parties through an 'Identity Attribute Exchange' as a successor to GOV.UK Verify.** As noted in Chapter 2, many companies already verify the identities of their customers. For example, when opening bank accounts (particularly in the FinTech sector), it is often necessary to scan your passport to create an account.[191] If companies have already

189. OIX, *HMG's Identity Innovation Dilemma*, 6 March 2019, https://openidentityexchange.org/networks/87/NewsTab_thread.html?-threadid=239

190. See recommendation 6.

191. Trulioo, *Identity Checks — Creating Quick and Secure Onboarding Processes*, September 2018, https://www.trulioo.com/blog/identity-checks/

checked identity documents, then there is no reason why they couldn't act as trusted identity providers in the future if they have verified the information provided by their users. The possibility of selling identity assurance to the Government would create an economic incentive for companies to adopt common standards.[192] Indeed, "the government LOA 2 standard for identity verification under GOV.UK Verify is equal to or exceeds the level of assurance currently achieved by the majority of banks in a non face-to-face on-boarding environment."[193] According to Computer Weekly, "as part of its planning for the government's future digital identity strategy, GDS has been working on a "trust framework" that aims to allow use of private sector ID systems within the public sector."[194] This would allow people to access Government services through 're-usable' digital IDs (see Chapter 1). Nonetheless, it may mean that the Government is unable to control the prices that it pays for an identity transaction and may also mean that private companies are left to determine who can and cannot access government services.

Recommendations

- **Preserve traditional methods of identity checks.** There are some individuals who either lack the skills or resources to access services online or who may always feel uncomfortable creating and using a digital ID. Although there has been progress in addressing the digital divide in recent years, the Government should acknowledge this fact and ensure that there is never a situation in which having a digital ID is mandatory or that certain public services are only accessible through the creation and use of a digital identity. To do so will assuage any public concerns about digital ID policy and will also ensure that public services remain accessible to all.
- **Create a dedicated ministerial portfolio for digital identity** At present, the Digital Identity Strategy Board will be chaired by officials from DCMS and GDS, which lead on digital identity policy for the private and public sectors respectively, and also include representatives from other departments such as the Department for Work and Pensions and HMRC.[195] The House of Commons Committee of Public Accounts found that "Verify's leaders demonstrated a poor understanding of accountability for the programme".[196] The Government needs urgently to set out its position on Digital ID and ensure that there is a clear relationship between, and accountability for, the various identity solutions being deployed across Whitehall.
- **The UK Government should publish a Digital Identity Strategy and 10-year roadmap.** It should aim to establish whether it is preferable for individual departments and agencies to design

192. See pp. 13-14
193. Open Identity Exchange, *How Digital Identities Which Meet Government Standards Could Be Used As Part Of Uk Banks' Customer On-Boarding And Kyc Requirements*, January 2017, https://oixuk.org/wp-content/uploads/2017/02/How-Digital-Identities-which-meet-Government-Standards-could-be-used-as-part-of-UK-Banks'-Customer-On-boarding-and-KYC-Requirements.pdf
194. https://www.computerweekly.com/news/252482828/HM-Treasury-tells-GDS-no-further-online-services-can-use-Govuk-Verify
195. New Statesman, 1 September 2020, https://tech.newstatesman.com/business/verify-2-0-industry-experts-cautiously-welcome-uk-efforts-to-overhaul-digital-identity-services
196. House of Commons Committee of Public Accounts, *Accessing public services through the Government's Verify digital system, 1 May 2019*, https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/1748.pdf

tailor-made identity solutions or whether it is preferable to use a cross-governmental platform like GOV.UK Verify. Focussing on the long-term delivery of a Digital ID strategy can prevent a situation where progress in the future is hampered by legacy IT problems. As the International Telecommunication Union noted any "Digital Identity Strategy should provide the overall Digital Identity direction for the country; express a clear vision and scope; set objectives to be accomplished within a specific time frame; and prioritise these in terms of impact on society, economy, and infrastructure."[197]

- **The Department for Work and Pensions should accelerate the creation of the DWP *Confirm Your Identity*.** The creation of a tailor-made identity solution for the DWP should be encouraged because those reliant on welfare are more likely to lack ID documentation. Nonetheless, there are clear advantages to developing cross-departmental identity solutions and there is a risk that every department will develop separate and siloed approaches to identity assurance, leading to increased costs for taxpayers.
- **Use the National Data Strategy to identify additional Government data sources that could be used to support identity proofing and verification processes.**[198] The digital availability of Government registers would support identity and eligibility checking. If digitised, these could be made accessible via API then it would be possible to use them for the purposes of identity verification.
- **The Government should create more nuanced identity standards and adopt them across all departments.** Forcing people to create a digital ID to a high level of identity assurance is necessarily time consuming and can discourage people from fully onboarding to a service.[199] Finding the balance between ease of access and the high levels of assurance that are often required to access Government services will be a key challenge. Nonetheless, it is important to remember that the primary function of digital ID platforms is - and should always remain - to prevent fraud. As a result, it is to some extent inevitable that there will be some friction in any identity transaction. GOV.UK Verify provided 2 different levels of assurance (LOAs) - LOA1 and LOA2.[200] It has been suggested to the authors that this creates an unnecessarily abrupt cliff-edge between levels of verification. A grading approach that is more refined may make it easier for cross-departmental identity solutions to meet the needs of departments and agencies, thereby improving pass through rates and making it easier to reuse digital IDs to access different Government Departments.
- **The Government should extend the scope of the Document Checking Service to include driving licences and increase participation in the DCS Pilot Scheme.** The Document Checking Service checks passport details against the HM Passport Office

197. ITU, *Digital Identity Roadmap Guide*, https://www.itu.int/en/ITU-D/ICT-Applications/Documents/Guides/ITU_eID4D_DIGITAL%20IDENTITY_ROAD_MAP_GUIDE_FINAL_Under%20Review_Until-05-10-2018.pdf

198. DCMS, *National Data Strategy*, 9 September 2020, https://www.gov.uk/guidance/national-data-strategy

199. Computer Weekly, *How to accelerate digital identity in the UK*, https://www.computerweekly.com/opinion/How-to-accelerate-digital-identity-in-the-UK

200. https://www.verify.service.gov.uk/understand-levels-of-assurance/

(HMPO) database. It provides a simple 'yes' or 'no' response to say whether a passport is valid without giving direct access to government-held data. The Government recently announced that they would be extending the DCS Pilot Scheme. In future, the number of private sector participants should be expanded dramatically, especially to include SMEs and emerging FinTech companies. Furthermore, at present it is only possible to check passport data against HM Passport Office data. The service should be extended to check other identity documents including driving licenses.

- **The Government should establish a trust mark for digital identity products.** Such a trust mark will be essential if the mooted Identity Attribute Exchange is to be successful. Rather than establish direct regulatory oversight of Digital ID services, the Government should try to set the standards for digital ID.[201] Creating a single Government regulator with the power and responsibility to examine every single company that wants to sell identity assurance is likely to come under significant pressure. It would be more effective for the Government to encourage companies to undergo digital identity compliance and information service audits delivered by private sector companies. Such audits could ensure not only that personal information is secure but also that verification checks are being performed to a sufficient level of assurance. Not only would such a regulatory model pass the regulatory costs from the Government to the private sector, but it would also be easier for the Government to regulate auditors against their statutory duties. There are already methods of proving that identity products are compliant with eIDAS, and the Government should explore how to expand this further.

201. See pp 47

£10.00
ISBN: 978-1-913459-41-3

Policy Exchange
8 – 10 Great George Street
Westminster
London SW1P 3AE

www.policyexchange.org.uk