Brought to you by Socitm Ltd | Reference: 21014

Report

Digital identity

November 2021

Socitm INFORM

Table of contents

Introduction

A national digital identity solution for the UK public sector has long been recognised as a vital element in modernising public services. For over 20 years, Socitm and its Local CIO Council have advocated such a solution to support not just the provision of truly people-centred services but also the shift to working with people before they get into crisis; prevention rather than cure.

Whilst the requirement for a solution has become ever more pressing, there has been a succession of failed digital programmes nationally, including the recent GOV.UK Verify system, on top of which these centrally-led programmes simply take too long and devour too many resources with poor returns.

Consequently, local government and parts of central government have given up waiting for a national system. In the face of growing demands they have been developing their own locally-based, digital authentication solutions. The problem with this is that the UK has now ended up with a patchwork of digital identity systems that typically are locked into service silos, are not shareable and are incompatible.

From the perspective of the public, in addition to having to understand many different methods of accessing secure public services online, this 'patchwork of solutions' has also been an unnecessarily costly journey for the taxpayer. Worse still, many of those who are digitally excluded find it increasingly difficult to access the very services on which they depend, especially during a pandemic.

But there is cause for optimism. The DCMS has been given a specific remit to develop a trust framework for digital identity that can embrace both public and private sectors. The vision is strong and compelling. GDS has stopped the Verify programme and has started with a new project that should be consistent with the DCMS framework. The NHS app is also an exciting development, showing the art of the possible.

And, most recently, the Public Service Delivery Board – a cross HM Government group, with Local Government Association (LGA) representation - has drafted a proposal for new legislation to enable data sharing for identity verification services, including those potentially offered by local authorities

More importantly the public, although cautious, appear ready to accept the concept of a digital identity, provided they are in control and unaccompanied by an ID card.

However, success will depend on any national solution recognising the complexity and diversity of local public services in how they are managed and delivered, not just focusing on the large transactional services of central government or the economic opportunities of the banking and retail sectors, although these are important.

A digital identity solution for the public sector needs to be able to address the more complex relational services typically offered at a local level, such as integrated health and social care, supporting troubled families, protecting children, driving equality, and reducing crime. It also needs to learn lessons from the past in terms of inclusivity and gaining high levels of public trust. This includes protecting everyone from digital fraud, abuse or unintended errors.

That is why this report is so important and timely, building on a local evidence base and describing what lessons can be learned from the past to improve outcomes for the future, with a local – people and place – rather than a central focus.

About this report

Focused on the application of digital identity in public services, this Socitm commissioned research presents a call for action founded upon research and evidence-based guidance for two key audiences:

- To provide a guide for those involved in digital public service design and delivery about the role and importance of digital identity to underpin future local public services provision.
- To support those involved in national policy and associated developments, particularly DCMS, GDS and the NHS, by presenting a clear and practical local perspective on digital identity, helping to ensure that mistakes of the past are not repeated in new national programmes.

We do not attempt to try to identify solutions to all the problems that have beset the UK in this area in the past. However, we do analyse the issues faced by previous digital identity programmes and offer insights into how they might be avoided in the future.

We also summarise the technology components that can form the basis of a digital identity framework for local public services (see Appendix A).

Finally, we set out a local perspective on digital identity for citizens, with examples and case studies described from the point of view of place-based service delivery (see Appendix B).

Please note that in this report we use the term citizens in the widest sense of the word to include all residents and those for whom formal UK citizenship may not be an option.

A bit of history

During the Second World War, cards were mandatory in the UK as a necessary proof of identity for rationing of clothes and food. They were accepted, although not loved, and were withdrawn in 1952, largely due to tensions between citizens and the police.

Since then, the UK has had a 'love/hate' relationship with identity systems, with the result that there are now many separate ID systems in place – vehicle licence, NHS number, national insurance number, passport number, to name but a few.

All of these could in theory have been unified, with huge potential value for local and central public services being integrated around citizen needs – improving services, saving money, reducing fraud.

Since the 1980s, as technologies have advanced, successive governments have attempted to introduce UK wide digital identity solutions for public services. On every occasion, programmes have been stumped by the difficulties in balancing risk and benefit, including the need to build public trust.

They were reintroduced in Britain by Tony Blair's Labour government in the Identity Cards Act 2006, largely seen as a response to the growing risks of terrorism. After failing in both delivery and support, the Act was repealed in 2010 by the Conservative/ Liberal Democrat coalition government.

The inability of the UK to introduce a universal digital identity, and the number of failed attempts to do so, has cost public sector heavily over the last 40 years. Unsuccessful national programmes have written off huge direct costs, while the opportunity of not having a solution, or waiting for one that never arrives, have arguably been greater still. Meanwhile, local authorities and various government departments have had to develop their own independent solutions or continue to rely on paper. The Scottish Government is embarked on its own Digital Identity Scotland (DIS) programme (see Appendix B).

On one hand, an ID system for public services can offer citizens freedoms and flexibilities - proof of age or entitlement, simple authentication, or just linking services seamlessly around individual needs. On the other hand, there are valid fears that it could be used to curtail those same freedoms and flexibilities – abused by governments, criminals or individuals and businesses with powerful interests - whether deliberately or through mistakes.

The interest in digital identity solutions to help the work of the security services and the police has caused public concern, as have the proposals to use citizen identification to share anonymised records with large companies for research purposes.

We can conclude that the challenges lie in cultural and design issues more than in the technology, while focusing more on the benefits to citizens than on value to service providers or security services.

Much hope rested on the successful delivery of GOV. UK Verify programme ('Verify' hereon in the report), which began in 2011. However, after ten years, this project has been terminated and a new single sign-on (SSO) and digital identity solution is being developed by GDS (see the history of Verify in Appendix B).

What is a 'digital identity'?

Few people can escape the need for (or existence of) a digital identity, whether it is to authenticate a payment for online shopping, to register for a service, or to prove identity when accessing public services or just using social media.

A digital identity is a digital representation of who you are, providing proof as necessary during digital interactions and transactions.

A digital identity is broadly any personal data existing online that can be traced back to you. It is not an ID card (but could be) and could simply be photos or posts on social media, your online bank account, search engine history and much more that identifies you. A national digital identity scheme is one that allows an individual's credentials to give authentication to multiple services and data. We all have digital identities, it's just very disparate!

It is not the same as an ID card, or a large central database of personal attributes and authentication methods, with a single identity number (although this is how a digital ID is implemented in many countries).

With the growth in digital services, and our dependency on them after the pandemic, delivering a unified digital identity for access to common public services has become increasingly urgent. Many services now depend on authenticated access for self-service, including those delivered by local and central government, health and in other related public sector organisations. Most people use a range of different passwords and other verification methods to gain secure access.

Access also extends to the needs of public service professionals, who increasingly work across their traditional organisational boundaries. This may be in virtual teams, in multiple employments/secondments or where employees from one organisation need to access data held securely in another. These conditions are particularly prevalent in local areas, where employees may move between different public service organisations as their careers evolve.

In each of these situations having a common approach to identity management can improve interoperability of public services and the way in which they work. Currently a great deal of time is spent creating temporary or new digital identity access for public sector employees as their work and professional needs change.

An agreed trust framework for digital identity management that allows public service organisations to use different technology for employee systems access, but based on common agreed standards, would potentially be both more flexible and more secure.

Whilst there are rightly fears over how digital identities will be developed and used, including being 'tracked' and whether they may drive inequalities, there is also no doubt that they can be safer, quicker, and easier than using a variety of physical documents in different situations.

At the same time, there are growing risks of identity theft, as well as risks that minority groups and individuals could potentially become excluded from access to services because they do not have a recognised digital identity (or don't trust service providers).

The key aspect of a digital identity is this it is trusted and understood by the public and by service providers. This report describes how this can be achieved, with a particular focus on place-based and integrated local public services.

One option is to produce a single digital identity trust framework of standards and regulatory control that can be used across public and private sectors alike, recognising that parts of the private sector, such as the banking industry, have had secure digital identity systems in place for some time.

DCMS is currently working on just such a trust framework, although it will not be easy to realise. For example, simply adopting a private sector model for the public sector is unlikely to work because needs and drivers across public and private sectors are very different. Local public services are often about solving complex social, economic, and environmental issues, and helping those most at risk. The private sector focusses on commercial transactions, such as retail and banking, whose customers are very different.

The DCMS programme

DCMS has been given the task of developing a trust framework for digital identity to be used across public and private sectors. It has been consulting on the approach to developing this framework, including with local government (see Appendix B).

For local government, what will be important is:

- How the solutions (policies, framework, standards etc) can work seamlessly across public and private sectors, without compromising the needs of the most vulnerable in society and without ignoring the most complex user cases that exist in local government.
- Ensuring that the solutions are sufficiently flexible to embrace the range of services provided by local government, not just being able to deal with the high-volume transaction areas of central government or retail and banking applications.
- Aligning NHS and other Whitehall digital identity initiatives (including the work by GDS) with the trust framework model from DCMS.

Notably, DCMS is not planning to build a solution, but rather to provide the necessary legislative, regulatory structures, standards, and governance for a robust and flexible trust framework, including an accredited governing body to oversee the rules and their implementation.

This should mean that different parts of the public sector, as well as the private sector, can develop appropriate implementations that work for them and have a common basis for compliance, interoperability, privacy, and trust.

This approach fits well with the recommendations and findings of this current research report. It also recognises that success in delivering a national public sector identity scheme has struggled to find a foothold in the past. The aims are clear:

> *"The plans laid out today will ensure people can trust the app in their pocket as much as their passport when proving their identity.*
>
> *Digital identities offer a huge opportunity to make checks easier, quicker, and more secure, and help people who do not have traditional forms of ID to prove who they are.*
>
> *This technology is a vital building block for the economy of the future, and we're ensuring that people who choose to use it can have confidence their data will be handled safely."*
>
> **Digital Infrastructure Minister**
> **Matt Warman, 19 July 2021**

At the same time, it will be essential that the GDS delivery programme of SSO learns the lessons of the past programme and aligns with the DCMS work (see Appendix B).

Improving delivery

The challenge of delivering a national digital identity scheme for the public sector in the UK is that arguably it is more complex than anything with which the private sector must deal. Nationally designed and delivered digital programmes in the UK have in many cases failed badly.

Part of the reason is that digital transformation is difficult, and the private sector is no different in the number of projects that fail – although often not as visible – as demonstrated recently by the Prudential digital upgrade meltdown.

But it is also true that certain problems have repeated themselves in national digital programme delivery, including:

- **Over-engineered or over-complicated solutions** such as the digital ID card scheme which conflated identity cards with digital identity mechanisms.
- **A centralised approach** where solutions are designed around high-transaction parts of central government and fail to understand the complexity of citizens' interactions with public services at a local level which always comes later.
- **Failure to resolve business case issues** and the commercial model for wider roll out, or the necessary standards, resulting in surprises later when costs escalate, and cost-recovery models emerge.
- **Poor design** where the different parts of the solution are not sufficiently separated, such as 'access', 'authentication', 'identity' itself and federated credentials, or the more complex needs of citizens are not understood.
- **Too great a dependence on the private sector** to have the solutions that will work seamlessly across the public sector or to overcome the programme complexities.

These are all issues with the failed Verify programme (see Appendix B). On the other hand, there are some clear strengths in the foundations for national government digital programmes:

- **Capability:** Some of the most capable, experienced, and talented individuals are involved, from both public and private sectors in major government IT projects.
- **Capacity:** The government has not underinvested in digital programmes that it has undertaken. It has employed the best people in the largest teams and engaged the top private businesses. The estimated cost of Verify alone was over £220m.
- **Vision:** Often centrally and narrowly focused, the vision may even at times be impractical in how delivery is envisaged, but Whitehall has some of the UK's best strategists and access to the world's best thinkers.
- **Too ambitious:** Sometimes the complexity is not fully understood (e.g. at a local level) but, in many ways, more ambition is needed. The UK lags many leading countries in terms of 'digital government' (despite the marketing messages), particularly because of its failure to address the digital identity of its citizens.

The key to success lies in the strengthening of governance and engagement:

1. Governance

There are plenty of groups, analyses, audits, scrutiny panels, reporting lines and consultation. But governance is often poorly executed in terms of wider involvement, accountability, continuity of leadership, and the ability (or willingness) to admit to problems, control slippages and intervene early.

2. Engagement

There is often a great deal of consultation, joint discussion and even cooperation between local and central teams. But true engagement, involvement, co-design and collaboration outside the central Whitehall 'family' often happens too little and too late.

These lie at the heart of the 'Socitm calls for...' from local government of central government colleagues working on national digital programmes relating to digital identity.

Digital identity: the calls from local government are clear

Central government, when developing national systems, recognises the value of local consultation, often with Socitm, the LGA and the Local CIO Council. If there is a criticism from local government, it is that involvement frequently is 'too little too late'.

Earlier and deeper involvement, especially to understand and reflect the complexity and diversity of local public service delivery, would be beneficial to local government but arguably also to the national programmes. Strategic visions, such as that underlying the DCMS-led UK identity and attributes trust framework, are much easier to state than to deliver in practice.

Unlike the Digital Identity Scotland (DIS) programme, which is being co-designed in collaboration with the full spectrum of public services, including local government, the scope of the GDS One Login programme is focused exclusively on UK central government transactional services and does not include local government. Further, it is unclear whether the lessons from the GOV.UK Verify programme have been fully understood and digested, including the ability to accommodate the socially inclusive, specialist and often complex interactions with local government and local public services in the potential rollout and adoption of the new GDS-generated solution.

Moreover, local government understands the complexity of some of the more challenging and diverse citizen circumstances, and these are often very different from the simpler but significantly higher volume transactional services delivered by central government departments.

Equally, there is a responsibility on local government to support national developments – providing time, ideas, and support wherever possible to help to overcome the more difficult political and cultural barriers, and to build public trust.

On behalf of local government, Socitm calls for:

1. Ensure that UK government resolves the current barriers to a unified trust framework for digital identity that encompasses the socially inclusive requirements of the local public services sector: including standards, legislation, regulation, resources, governance of identify providers, audit, and compliance checks.

2. Seek investment for local government to build a sector specific capability for local public services that is interoperable with national solutions: in the confidence that this will be approved and trusted in accordance with the UK identity and attributes trust framework , GDS One Login programme, and Digital Identity Scotland (DIS).

3. Be involved in the design of policies, architectures, and principles, not just consulted on a design or prototype model. In other words, to de-risk the design phase, local government needs to be represented 'inside the tent' as part of the design, development, and deployment team.

4. Ensure that the development starts with the end user. This means avoiding the 'developing first for Whitehall and then generalizing' approach, which does not reflect diverse citizen needs. Notably, there are a range of local issues and business requirements that

are unique and need understanding early. This includes ensuring the needs of excluded groups and individuals are considered first not last.

5. Ensure that the citizen is always in control once their identity reference is established – they can choose to allow their authentication to be shared with other services, or data linkages to be made, or data shared for whatever purpose, and can easily see what data is held, what linkages made and how to adjust these to ensure it is only ever 'by consent'.

6. Ensure the design is both modular and adaptable. This means separating out components such as the identifier structure, access methods, authentication, and electronic data sets/records design, rather than conflating them. Adopting the DCMS trust framework for example.

7. Design identity solutions and services in such a way that the access can be made truly frictionless for the local service user, including those who do not have a mature digital footprint (following the GDS design principles rather than just stating these as policy ambitions).

8. Build in adaptability and flexibility in the design for future applications and use, rather than seeking to develop a comprehensive set of 'patterns' that can cover the full range of local user cases is neither affordable nor sustainable. In particular, giving the 'blueprint' to local government to use to develop local implementations with a confidence of compliance and compatibility.

9. Be transparent about the business case, and commercial arrangements of any solution, and on-going business model, so there are no surprises. This includes being part of and involved in signing off the business case. This was a key failure of the Verify programme and its inability to authenticate the majority of users.

10. Openly list and agree the issues associated with the first Verify programme, so that there is transparency and honesty in how the barriers and problems will be addressed in any future development.

11. Ensure that any other digital identity initiatives across Whitehall are aligned to the GDS and DCMS, including work in the health sector. If a common approach cannot be prioritised across central government it will be harder in the wider public sector, with incompatibility and weak interoperability adding costs, risks and barriers to local, placed-based digital services. Ideally citizens will be able to track all their dealings across public services.

12. Ensure technical interoperability, with recognised and agreed standards, open APIs that will allow future connections and linkages to be made by councils when required. This includes ensuring that a 'proof of identity' secured by a citizen in one public service can be shared and is portable across others – if the citizen chooses (allowing differing levels of authentication, with a seamless movement from one level to another for a citizen, as they access different and related public services).

13. Ensure cyber protection and resilience have the highest design priority, with transparency and control resting with the end-user as far as possible. Wider public trust will be essential if local public services are to adopt the model from the centre. This includes ensuring that solutions are simple (or familiar enough by replicating existing methods in public and private sectors where appropriate).

Download our infographic here:
Digital Identity infographic

Harmonising local and national drivers

National IT projects in the UK have tended to focus on high volume transaction areas undertaken by a variety of government departments – HMRC and digital tax, DWP and benefits systems, and DVLA and car tax/licencing.

These transaction areas are very different from those in local government, where relational services are particularly critical in supporting citizens in areas such as crime prevention and responses, environmental pressures, land use planning, health and social care integration, homelessness, multi-generational unemployment and troubled families.

It is therefore almost inevitable that there will be subsequent difficulties in retrofitting national solutions to local government, with its complex mix of relational services and clients with specialist and complex needs. Sometimes national government believes that there could be 'one local government website' – but this is to fundamentally misunderstand the function and activities of local public services.

This is not to say that local digital identity system solutions do not depend on a nationally-led trust framework, but, leaving the design implications of embracing local government services until later, results in limited reach and range of digital services suited to the framework.

Some of the more complicated cases are associated with vulnerable citizens, often with limited digital capability. There may be a need to accommodate multiple identities for example, in situations where, say, 'household' is not the same as 'family' or 'address'.

The solution to digital identity and authentication to services needs to be more flexible at a local level than is likely to be required at a national level. Common standards and architectures, co-design and when necessary, master data management and data matching tools can help to ensure harmonisation is possible, allowing authenticated certificates to be passed between public services as required (see figure 1).

Why now?

The UK public service sector has had a need for a universal digital identity system for many years.

Socitm has lobbied for this to be a high priority for the Cabinet Office and the Government Digital Service (GDS) to develop since the early 2000s, arguing that a common approach to citizen identity and authentication, based

Figure 1. Co-creation of digital identity solutions for local public services harmonised with a national trust framework

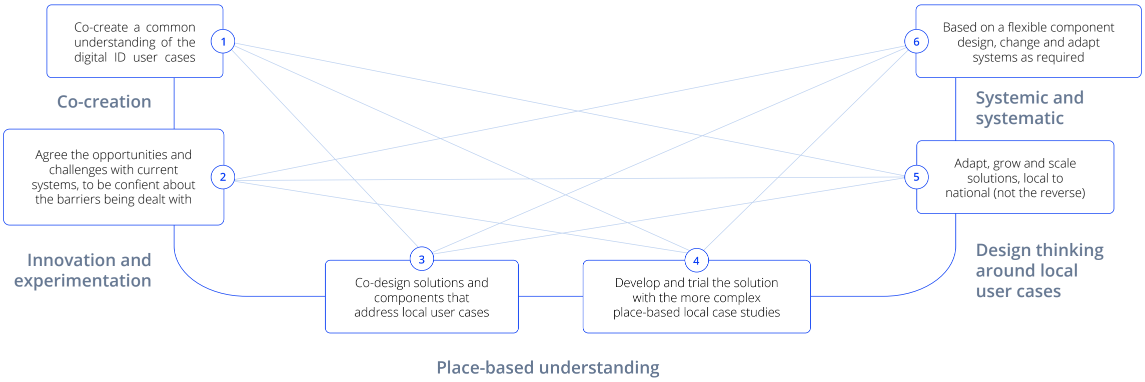
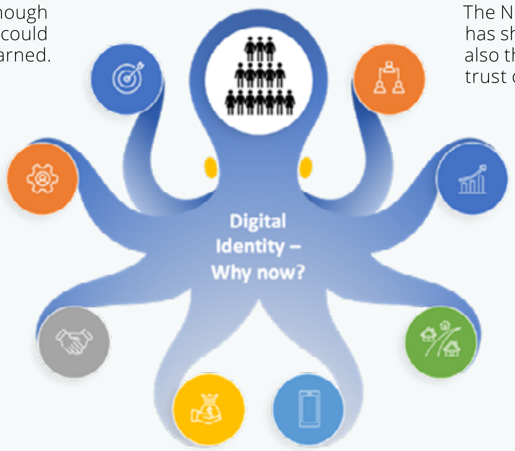

Co-create a common understanding of the digital ID user cases
1
Co-creation
Agree the opportunities and challenges with current systems, to be confient about the barriers being dealt with
2
Innovation and experimentation
3
Co-design solutions and components that address local user cases
4
Develop and trial the solution with the more complex place-based local case studies
Place-based understanding
6
Based on a flexible component design, change and adapt systems as required
Systemic and systematic
5
Adapt, grow and scale solutions, local to national (not the reverse)
Design thinking around local user cases

Figure 2. Digital identity – Why now?



Experience
Verify and other programmes, although unsuccessful, have shown what could be achieved, if lessons are learned.

'Track and Trace'
The NHS track and trace system has shown the possibilities, but also the imperative nature of public trust of any national system.

Technology advancement
Technology progress offers new opportunities for digital ID solutions, protects citizens, joins up services and places the citizen in control.

Other countries
The UK is falling further behind on digital developments because of a lack of digital ID. Many countries have solutions, and have shown what is possible.

Integrated care
Integrated care systems (ICS) depend on a shareable digital identity spanning more than just health, and this is a high priority.

Local needs
Local government is pressing for a solution nationally and is supportive of national standards. The benefits are clear to public services and citizens alike.

Business
UK productivity, as well as the ability to compete in a global market, can be shown to benefit from an additional IT solution that works for the private sector.

NHS app
The NHS app has been launched and widely taken up, because of the vaccine 'passport' possibilities, and is now being trialled in Manchester for local public services more widely.

on open standards and shareable authentication, would save huge amounts of wasted effort, improve the join up of local public services and protect individual citizens.

There are many examples across the public sector where an identity verification process is necessary, with different levels of authentication. In local government many requirements are for lower levels of authentication, (such as renewing a library book), but most of the 700 or so services for a unitary council would benefit from user-authenticated access, to provide a better service.

Currently there are a myriad of identities, access methods and authentication approaches being used, which adds cost, complexity, and challenges for citizens – as well as, arguably, cyber risks of multiple credentials. Common standards and a common approach would allow this to be joined up and shareable reducing the need for a continued reliance on paper, with the costs and inherent risks that that implies.

Despite the past problems and public scepticism about developing a digital identity system for the UK, there are several factors that have come together that make this the best moment to develop a nationwide solution, perhaps more opportune than at any time in the past (see figure 2).

Is the UK different?

Most countries have a digital identity system in place for citizens, working successfully, accepted by them, and not abused.

Today, there are only two countries within the European Union that do not use any form of identity card: Ireland and Denmark – with all other members of the EU using some form of ID card scheme, whether optional or mandatory. The cards in the EU typically are used for service access, proof of identity for things like age verification and freedom of movement.

At the end of 2020, digital identity schemes were interoperable in Europe in 14 countries: Germany, Belgium, Croatia, Denmark, Estonia, Italy, Spain, Latvia, Lithuania, Luxembourg, the Netherlands, Portugal, the Czech Republic and Slovakia. The UK's Verify programme is the 15th – but not considered operational.

There are many differences between these countries and their approach to citizen identity:

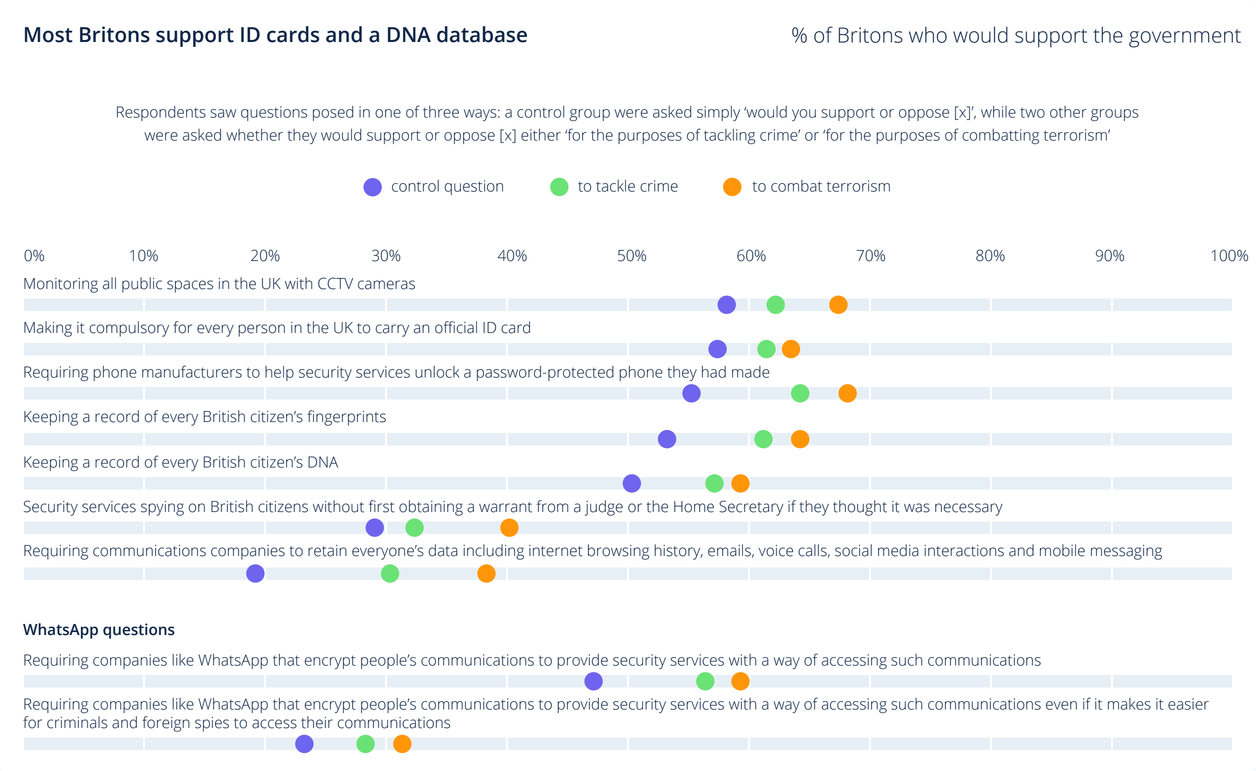
- Some are enforced by governments with little option for citizens but to comply. Often the purpose is to benefit the state, rather than to benefit the citizen.
- Countries vary in their acceptance of the concept of a state-wide digital identity, often because of their history, size, culture and geographies.
- Technologies used vary from a basic number identity system to the use of biometrics.
- Many ID cards have differing purposes (usually related to security), while other are broader digital identity solutions linked to a card.

The UK public has higher anxiety about identity card use in a democracy than other countries, with a majority holding concerns over privacy, the perceived loss of personal freedoms and the fear of the UK becoming a "police state".

A focus on using identity systems to prevent illegal immigration (a Brexit topic of debate) or to help the work of security forces to prevent crime, has fuelled concern, rather than found populist appeal. These concerns include:

- A deep inbuilt fear about 'ID systems', coupled with a lack of trust in governments. It is a worry in the UK that any national ID system would be a risk; subject to potential abuse or controlling or limiting the very freedoms it promises to enhance.
- The size of the UK, the diversity of its citizens and therefore the complexity of any unified single digital identity solution for all services, public bodies, and citizens.

Figure 3. 2018 YouGov poll, Most Britons support ID cards and a DNA service



- The competence of successive UK governments to deliver complex digital projects, especially in identity systems.

These barriers can be overcome, but a new approach is required. Focusing primarily on the benefits that a digital identity system can bring to UK security, immigration control, and public protection, whilst appealing to governments only adds to public concerns and distrust. The government should instead focus on social value, economic benefits, and public service improvements that could be achieved, building on the support that has been found from the UK public in surveys, where the majority would appear to be in favour of some form of recognised and trusted identity system.

For example, a YouGov poll in 2018 found that most of the UK would be in favour of introducing ID cards (see figure 3).

Estonia has successfully introduced an all-embracing digital identity system which underpins joined up digital government services and is often cited as an example which the UK could follow. 98% of citizens in Estonia have a digital ID card, linked to a variety of smart identity services from government, to improve business efficiency and equality of access, and enabling proactive public service delivery.

Arguably, Norway is another example for the UK to consider in developing its own digital identity solutions, in particular because it has moved away from an ID card to a more general system linked to banking. Norway has had several attempts at introducing a universal system before the current service was rolled out.

However, both Estonia and Norway are very different from the UK, culturally and in scale. Neither Norwegian nor Estonian citizens can easily opt out of the national identity systems in their country, and both countries are of course much smaller than the UK, with greater homogeneity in government activity, purpose and service delivery. The loss of anonymity is accepted and trusted because of the significant benefits that digital identity provides to their citizens (see figure 4).

Figure 4. Benefits of an ID card in Norwey and Estonia

The Norwegian identity card is a non-compulsory biometric system launched fully in 2020. It sits alongside the Norwegian passport and is only issued to Norwegian citizens. It is used as an authentication mechanism for a whole variety of government and public services, such as fully integrated bus travel across the whole country, or when necessary to prove identity for other purposes.

It is linked to bank accounts and supports authenticated payments. It is connected to the tax system, medical records and insurance and citizens can login to see their details – what information is held, how it is used and status of pay, tax, medical records and more.

The Estonian national identity card links 5,000 separate electronic services. Citizens can enter into agreements, sign documents, submit various applications, use digital channels and communicate with various state authorities.

The chip on the new card carries embedded files, and using 2048-bit public key encryption, it can be used as definitive proof of ID in an electronic environment. It was upgraded with new security in 2018, with a colour photo that only appears when viewed from an angle. One new detail is the inclusion of a QR code, for faster validation.

The UK needs to focus

There are many examples recently of attempts to introduce digital identity in the UK. The most recognised, was the Verify system (now terminated but moving to a new version – single sign-on [SSO] and digital identity system).

Other past examples include the ID Card programme in the early 2000s, a variety of NHS programmes focussed on electronic patient care records and a solution from the Department of Education 20 years ago which almost succeeded and was shared in parts of local government.

Some of the national UK Government digital identity programme examples at the time of writing (and there may be more) include:

- GDS's 'identity and attributes exchange' and SSO programmes
- The NHS app
- DCMS consultation on a framework to create a range of standards and regulations intended to enable interoperability of government and industry
- DVLA digital identity scheme
- Home Office EU Settled Status Scheme
- DWP Government Gateway replacement service (and Gov Gateway itself)
- HMRC Identification verification system (because they could not use Verify)
- Digital Business Identity Scheme from the Department of Business, Energy, and Industrial Strategy.

This list does not include the range of existing authentication methods across the public sector, some based on the Government Gateway service that has existed for some time. The growing range of digital identity programmes falls into two categories of drivers:

- **National projects started by national bodies**, including the NHS and government departments in particular. Many of these do not seem to be joined up, or are deliberately competing in order to optimise a solution based on a specific set of transactional priorities.
- **Local solutions**, typically initiated by local government, in the absence of any national solution yet being in place. These examples include such things as 'my council, 'my account', 'my local app' and so forth.

It is impossible to hazard a guess at the cost of the diverse range of UK initiatives over the last 20 years or so, or the opportunity costs that have been missed because of projects that have failed, but it is likely to be £billions of taxpayers' money.

There is nothing wrong with the concept of having different log-on and security management systems for different services and organisations. This would work particularly well for local authorities with a huge and diverse range of services. However, harmonising the underlying standards and methods for different levels of security would allow portability of credentials where appropriate, and commonality of structures and technologies where possible, simplifying service access and reducing cost overheads.

Ideally, building on the concepts from the DCMS, the UK government would focus its energies on creating a single, recognised trust framework that individual public service organisations could consume and reuse.

Standards and standardisation

There is a logical argument in favour of connecting all public services together with a single unique identifier. This would enable citizens to connect related services together, as they require, and to reduce the overhead of multiple IDs and the associated authentication systems. Indeed, this is what countries such as Norway and Estonia have achieved.

However, there are some significant drawbacks to this:

- It would present huge challenges in terms of the scale of changes required in the UK.
- The cost would be enormous, with questionable value in some areas.
- There are political, technical, and commercial challenges to overcome.
- Resistance from some parts of the press would arguably be enough to sink the endeavour before it started.

It follows that a distributed solution based on a common framework of standards may offer the best way forward.

Digital standards have been problematic for the UK government. GDS has promoted its own preferred standard for Verify (Good Practice Guide 45) and DCMS (now the lead government organisation for common digital identity) is developing a digital identity trust framework in parallel. Hopefully, these will be harmonised through their design processes.

There are also recognised standards for digital identity in the private sector. Development of Verify was ultimately reliant on the private sector delivering solutions based on recognised standards.

The DCMS trust framework, currently under development, consists of a range of standards and regulations intended to enable interoperability of government and industry identities. The ambition is to allow a digital identity created by a recognised private sector provider, such as a bank, to be used to access online public services, and vice versa.

This approach reflects that advocated by the Open Identity Exchange (OIX), as GDS's preferred identity standards body, that seeks to accelerate the adoption of digital identity services based on open standards across the private and public sectors, recognising the challenges of reconciling the tensions between public and private sector interests.

The problems associated with standards, let alone standardisation, need to be resolved by GDS and DCMS working together, involving local government in the dialogue before any firm decisions are taken. The opportunity is for the whole of the UK government to work together to join up the existing range of initiatives into a single identity systems architecture, embracing health, local government, and national government services.

This does not mean a single 'all-embracing IT system', but rather an architecture that consists of a set of standards, and policies based on four key principles:

1. Operate on a distributed basis

...not a 'big central database' or single login that could be abused or hacked as a whole, supporting the need for identity portability across the wider public sector.

2. Place the citizen in control of access, data and linkages

...a fundamental design principle and the starting point of all digital identity system developments (and their components).

3. Build on a modular basis

...so that the different aspects of access, authentication, identity management and digital records development are separated, to create simplicity, protection and adaptability.

4. Make provision for the digitally vulnerable

...understanding and including in the design process those that are digitally excluded. This means ensuring that those who are fearful or less capable of using technology are adequately supported and involved.

This would allow local authorities, for example, to use a common digital identity design with recognised and agreed standards for citizen verification, enabling the sharing of a persistent identifier so that:

- **Local verification can be shared**, and support given where required to encourage and maximise take up.
- **Past transactions can be held, shared, and linked** to avoid the need for the public to constantly repeat their story.
- **Digital services can focus on the more vulnerable members of society**, those at risk, those in need of extra support and those falling behind in terms of digital maturity.

Overcoming public concerns

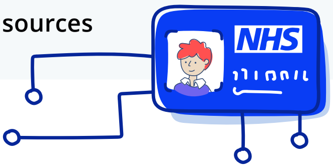
The challenge for the UK is not just to address citizen fears over a digital identity system. There are also differences in political views, strong press interests, concerns from pressure groups, academics and professionals, for example in health, while the private sector seeks to protect its commercial interests. This is a complex issue, and there will be many people (often older voters) who will never feel comfortable with being part of a national digital identity system.

Professionals' interests, from the technology sector and other specialist areas, such as education, health, and security services, are often powerful lobbies. If UK national identity programmes are going to succeed, their views need to be heard and reflected. Conflating digital identity with digital records is a specific problem – such as linking the NHS authentication mechanism in its app to digital records, which could then be shared with the private sector or across different parts of government.

The NHS track and trace system has shown how quickly a system can develop public distrust if mistakes are made. As the third wave of Covid infections rose in July 2021, nearly 0.5 million people were 'pinged' to self-isolate, even where the actual risk and contact was low. The result was a mix of lost working hours and many switching-off or deleting the app.

Many citizens accept the benefit of an identity system which offers real and new value (often younger voters). They recognise the increasing value of having some form of digital identity to make life easier and are often less concerned about the potential risks.

Figure 5. Digital ID access to NHS information sources



- Letters
- Hospital records
- Test resuls
- Core plans
- Email
- Systems data
- Recorded conversations
- Condition data
- Microfilm
- Medical history
- Video
- Related diagnostics
- Paper
- Service performance
- Metrics
- Social care records
- X-ray plates
- Free format data

Reconciling these two perspectives demands transparency and trust:

- How data will be held, used, and shared, and ensuring that citizens remain in control and can easily see the data held about them and where it is being used.
- Care in how any data is 'sold on' or shared with businesses, even in anonymised ways for legitimate research purposes (such as Google and Facebook).
- Avoiding the message that 'digital identity' is the same as an ID card, especially one whose main purpose is to control and protect.

- Keeping transactions, records, identity itself and attributes separate, with the linkages under the control of the individual citizen.

But achieving these aims is not straightforward. The complexity and range of data potentially being connected is difficult to explain, taking health data as an example of the diversity of content and interactions (see figure 5).

Data ethics, privacy and cyber safety

The main concerns that people hold about building a national digital identity come from worries about its potential abuse - intentional or otherwise.

As cyber criminals (and technologies) become more sophisticated, so the risks grow, and digital identity theft is now one of the biggest sources of global crime: fraud, manipulation, impersonation, extortion, and abuse. The deeper the identity works (such as across services, integrated with AI engines) the greater the risks and the potential impact.

As digital services and working increase, the public sector has a duty of care not only in the way that it develops identity solutions and citizen facing applications, but also by providing support and setting a standard for others to follow.

The UK should set an international lead in protecting data, privacy, and security from cyber threats in the way digital identity solutions are developed and used. Arguably, this lies at the heart of modern democracy and equality, and can be a significant competitive advantage for 'UK plc'.

Indeed, done well, the digital identity system can protect individuals, communities, services, and data in ways that a paper-based and partial digital solution cannot. It can enhance democracy, give a voice to those who are currently unheard, and limit the power of big companies to dominate the views and actions of communities.

GDPR goes a long way to protect individual rights and could be developed further to underpin and protect society against the risks of an abused digital identity system. For example, a digital ID system for public services must:

- Not be compulsory, and by not joining, or limiting use, the restrictions are clearly defined for the citizen
- Be usable by all, in all circumstances, alternatives put in place, without barriers in cost, technology or complexity that excludes minorities
- Have clarity of accountability for abuse, errors or poor practice by service providers, with necessary governance and national oversight
- Include clear mechanisms for human intervention when necessary to provide support, guidance and resolution of issues affecting individual citizens
- Adopt specific and recognisable methods for preventing and dealing with fraud, reducing the risk and impact of identity theft and other problems associated with digital identity
- Not be used in ways that are not anticipated, expected or are not under the citizen's control, with transparency of personal data use in particular
- Include the necessary levels of security, privacy, data protection from the simplest transactions to the most secure, published and transparent
- Ensure that personal data is never shared or sold, or in any way reused without knowledge and agreement of the individual, and care is taken with anonymised data in particular
- Preserve specific access rights for public protection agencies such as police and social care, but that these are strictly defined and limited, and are not the main drivers for adoption.

Socitm has already undertaken a range of research and publications on digital and data ethics and that work can help to underpin any national digital identity scheme.

NHS in the vanguard

We are all familiar with having an NHS number – it is a long-accepted ID number that provides a unique connection to health services and personal health records. It is accepted because it has a single and defined purpose and delivers essential value to patients.

In addition, the NHS is in general trusted by the public, and citizens feel comfortable about digital health data (within limits). This is shown by the recent development of the NHS app, developed by NHSX, the digital team supporting the NHS modernisation programme.

The app seeks to simplify patient access to services, connecting patient records, needs and other data. It seeks to reduce or even to eliminate the need to repeat information at every visit to a hospital, consultant, outpatient clinic or GP. It is in fact a leading digital identity system for public services, without a physical ID card (see Appendix B).

Although it is somewhat cumbersome to register initially, it does give access to a range of personal health data, including Covid-19 vaccination status.

The personal Covid vaccination confirmation within the app is driving take-up, not because of the health benefits of the app in general, but because this certificate of vaccination potentially offers citizens the ability to travel on holiday abroad or to gain access to events and hospitality.

While its original purpose was to harmonise and to digitise health records, its success in take-up lies in the wider value that it can potentially bring to UK citizens, along with general trust in how data is held and used.

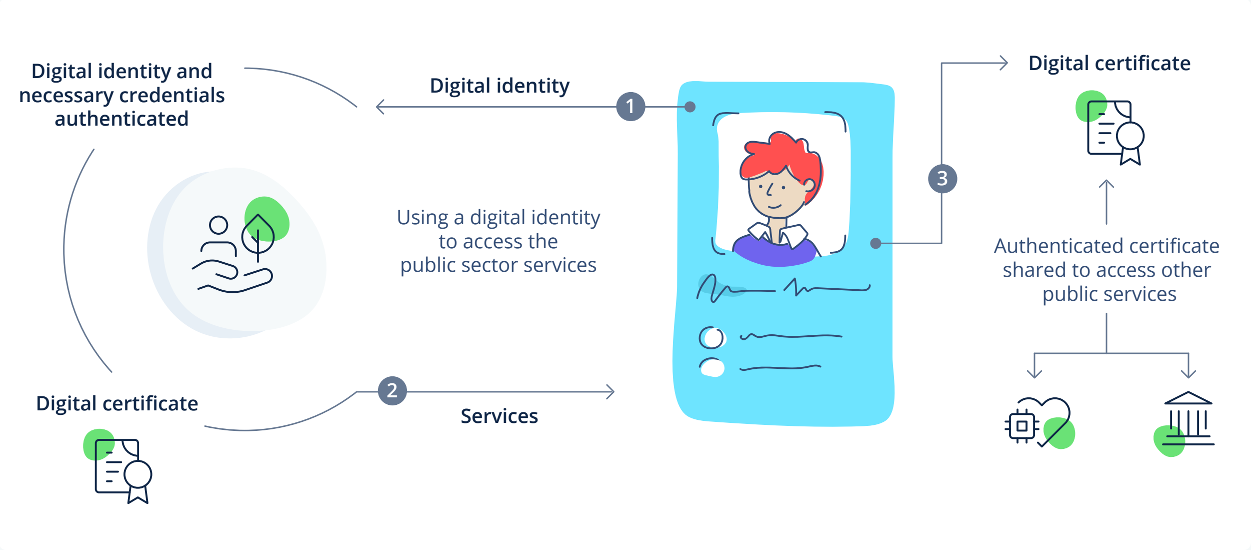
The future of healthcare lies beyond the boundaries of a hospital building or GP practice. Health data and services will typically be distributed, and digital methods will be essential to ensure access, authentication, and data linkage:

- **Data will be held by multiple organisations**, and on multiple types of devices, including by the individual on wearable devices and implanted sensors. That data will not just be medical diagnostics, but a range of care-related data, which collectively helps to support the well-being of an individual.
- **Services will typically be distributed** much more than they are today, across GP practices, different types of hospitals, and community care. In China, there are already virtual hospitals with no physical hospital building, but rather a digitally interconnected mesh of specialist and outpatient support services.

Any digital healthcare identity solution must be fit for this future and adaptable for wider use in a distributed environment, well beyond current NHS services, whilst at the same time adhering to commonly recognised standards and principles for identity management and protection of individual rights, privacy, and data protection.

Figure 6. the NHS app

Figure 7. Digital identity services


Digital identity and necessary credentials authenticated
Digital identity
1
Using a digital identity to access the public sector services
Digital certificate
2
Services
3
Digital certificate
Authenticated certificate shared to access other public services

Portability and sharing

One of the benefits of common digital identities based on recognised and accepted standards is the ability for that identity to be shared across public services, if the data owner wishes (the owner being the citizen, not the public body which is the custodian of citizen data – although they may seek authority to share in the citizen interest).

Once trust is established, the certification of access rights should be reusable with similar levels of authentication, avoiding the need for complex re-authentication for related services. For example, if you are fully authenticated on the NHS app, this should be sufficient as a method of identity recognition to be used in most if not all local authority secure transactions.

This will allow the same credentials to be used to log into different public services, if the citizen wants, without having to repeat the same initial authentication and identification checks every time.

Or it might be about data associated with the individual citizen account being shared between different departments in a hospital, or between a hospital and social care, or with benefits agencies such as Universal Credit. This would especially help those in need of a multiplicity of public services that need to be linked (see figure 7).

This process should be controlled by the individual who chooses to allow the connections to be made, because they know they will be receiving improved services that benefit them as a result. It should always remain an option to be able to log in securely and separately to each service individually, if preferred.

There are notable exceptions where public authorities can be allowed to override the individual; in the case of suspected fraud, criminal activity or where vulnerable people are at risk. In these situations, specific protocols are required to ensure that data linkages and connections are used appropriately, with the necessary authority and approval, and within the defined statutory obligations and limits, for both privacy and protection.

One of the more difficult areas is when public bodies wish to share anonymised or pseudonymised data with other organisations such as academic and research bodies, charities, and pharmaceutical companies, all of whom have a potential interest in the data and can provide new insights to guide policy development. Sharing data in this way can also bring in new investment from the private sector to the public sector, as well as shared technology innovation.

Even when data is anonymised, there will often be public concern and professional resistance. As a principle therefore, the benefits should be openly and transparently explained to avoid undermining the public trust on which success of any digital identity framework depends.

Many of the same principles stated elsewhere in this report should therefore apply:

1. **Digitisation of records and identity are different:** Unifying digital identity does not legitimise records being digitised or shared – this should be treated as a separate topic and project (as were 'digital identity' and 'identity cards' in the early 2000s – see Appendix B). Failure to recognise this may undermine public trust.

2. **Control by the individual is paramount:** Connection of data records should always be in the control of the individual. It should be the prerogative of the individual citizen or patient to consent to records being linked and to be able to cancel that authorisation at any time. This will oblige public services to persuade the individual of the value of any data linkages.

3. **Data sharing for research and other purposes is up to the individual:** Sharing data for research and other purposes should also be under the control of the individual. Pseudonymised data is often not sufficient in all cases to protect individual data, especially when sophisticated artificial intelligence and data insight tools are deployed with linked data.

4. **A personal digital dashboard is needed:** Citizens and patients should be able to access a personal digital dashboard, to view what data is held about them by public bodies, and where sharing consent is in place.

Citizen in control

For all the criticism of the big technology companies such as Facebook, Apple, Google and Microsoft, all of these allow individual users to select the degree of openness, data sharing and privacy (albeit not easily at times).

This must be the starting point for UK government systems, which need to go significantly further in terms of transparency and trust, setting an example to the private sector, but also potentially to the rest of the world in digital ethics and identity.

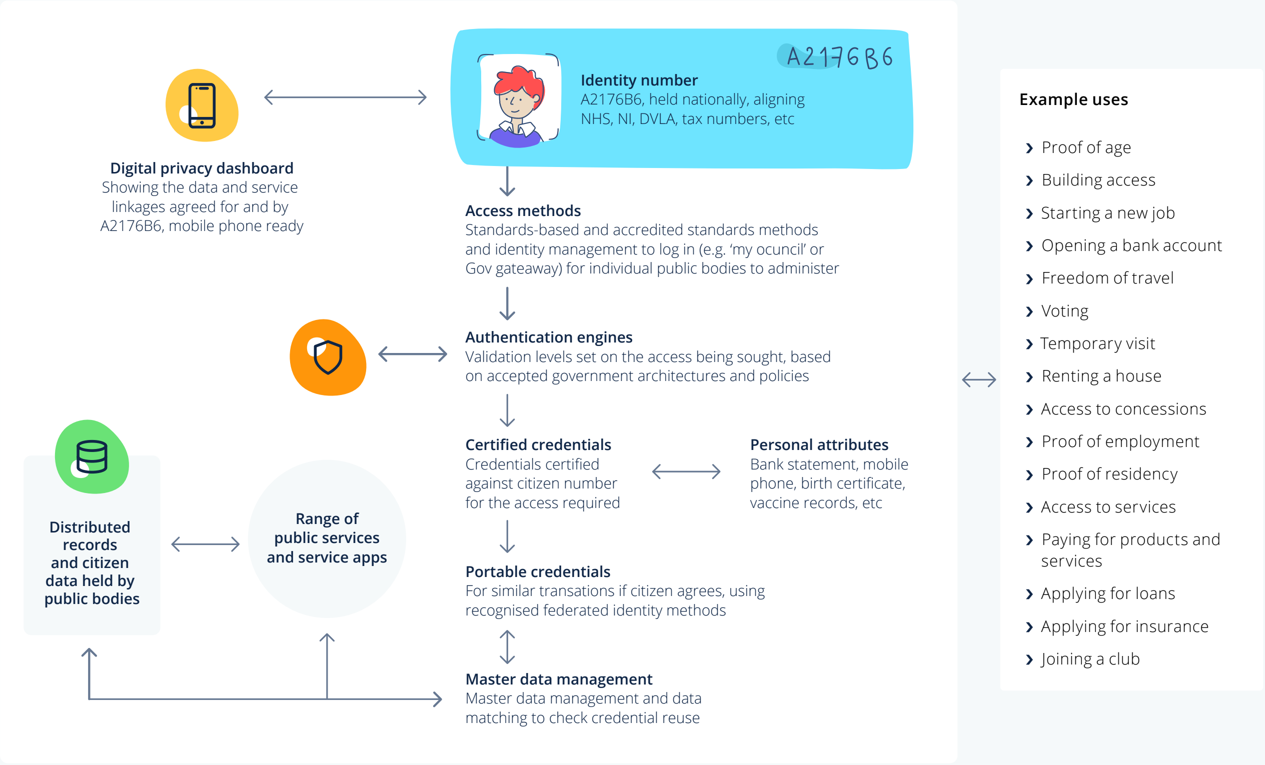
Under GDPR, citizens already have subject access rights, allowing them to find out easily what data is held about them by public service organisations. But to develop a single harmonised digital identity solution for the UK more would be needed; building a common architectural design that allows data sets and identities to be linked across services with an irrefutable personal 'ID' that is capable of reuse for secondary purposes is not technically that difficult to design, but it is not easy to deliver in practice:

- **Harmonisation:** A unique identity should ideally be harmonised across health, national insurance, tax, social care, benefits, and other areas. However, this does not all need to be achieved in one go, and prioritisation is needed, probably starting with health as the main lead.

- **Citizen conversation:** Citizens should be asked how they want service connections to be made, in their interests, by the public service provider. In other words, they can choose how far they allow the harmonisation to go.

- **A digital dashboard:** An online digital dashboard should be developed that allows an individual citizen to see the connections made between their data and different services, and to automatically switch them on and off as required.

Figure 8. Accessible, user-controlled structure



Identity number
A2176B6, held nationally, aligning NHS, NI, DVLA, tax numbers, etc

Digital privacy dashboard
Showing the data and service linkages agreed for and by A2176B6, mobile phone ready

Access methods
Standards-based and accredited standards methods and identity management to log in (e.g. 'my ocuncil' or Gov gateaway) for individual public bodies to administer

Authentication engines
Validation levels set on the access being sought, based on accepted government architectures and policies

Certified credentials
Credentials certified against citizen number for the access required

Personal attributes
Bank statement, mobile phone, birth certificate, vaccine records, etc

Distributed records and citizen data held by public bodies

Range of public services and service apps

Portable credentials
For similar transations if citizen agrees, using recognised federated identity methods

Master data management
Master data management and data matching to check credential reuse

Example uses

- Proof of age
- Building access
- Starting a new job
- Opening a bank account
- Freedom of travel
- Voting
- Temporary visit
- Renting a house
- Access to concessions
- Proof of employment
- Proof of residency
- Access to services
- Paying for products and services
- Applying for loans
- Applying for insurance
- Joining a club

- **Digital inclusion:** Specific design priorities should include the needs of those who are digitally excluded or who have concerns about their digital profile or are simply excluded for other reasons such as health, education, minority status, economic position, or language.

'Digital' versus 'technology'

It is easy to get submerged in the technology necessary to support digital identity. Indeed, the government's own consultation documents that have been recently circulated on digital identity plans (DCMS and GDS) focus heavily on technology and as a result difficult to fully grasp for the uninitiated.

Clearly the technology matters, but it is more about how the technology should be applied rather than how the technology will work. Technology is not the main barrier to a successful framework for digital identity. It is answering questions about why it is needed, and how it will impact individuals and organisations that matters most.

This report advocates a modular, distributed, citizen-led, and standards-based approach. It is more complex in practice than a single solution, particularly to deal with exceptions in terms of specific services or individuals, and it requires an accessible, user-controlled structure (see figure 8).

More background on the technology components relevant to this report are described in Appendix A.

In practice, an individual may legitimately have different identities for different purposes. A digital identity solution must be able to accommodate multiple purposes in multiple different scenarios – work, home, leisure – as well as different degrees of security requirement based on the nature of the transaction or interaction.

Conclusions

This report seeks to help public service professionals in developing a common approach to digital identity across the public sector. It recognises the need to balance the interests of those public service organisations in supporting the needs of the public, and the individuals themselves who have the most to gain and lose.

Overall, we conclude that there has never been a better time to develop a UK-wide digital identity trust framework. There is a substantial degree of public support, political will, business necessity and technology opportunity waiting to be harnessed.

The work of both DCMS and the GDS offers optimism for the future, alongside development of the NHS app and the parallel work going on in Digital Identity Scotland.

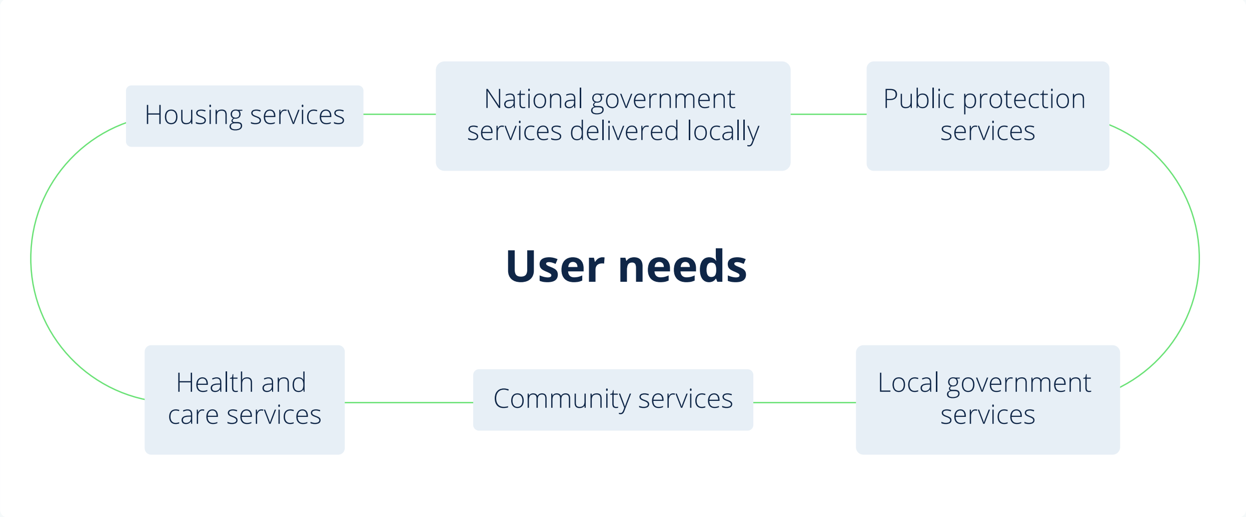
Mistakes of the past need to be publicly acknowledged and reflected in the way new solutions are developed. This is particularly true in the way that local public service needs are reflected in any national solution.

A trust framework approach, which allows digital identities to be used, shared and managed by an individual and by an individual organisation, with modular and reusable components offers the best way forward for complex local needs.

This requires more than just consultation and involvement from local public service organisations in national developments. It means that the framework should be designed from the outset to reflect the diversity and complexity of relational services at a local public service level, not seeking to retrofit these complex user cases in a national system designed primarily for high volume transactional areas of Whitehall departments.

Local government operates within a local ecosystem of public services, where a common digital identity architecture could embrace a variety of locally related services used by individual citizens, with autonomy at a local level conforming to national protocols (see figure 9).

Figure 9. Trust framework of interoperable access


Housing services
National government services delivered locally
Public protection services
User needs
Health and care services
Community services
Local government services

Appendix A

The technology behind digital identity design for public services, with associated security credentials, authentication, and access mechanisms, is complex. It is an order of magnitude more complicated than developing a single system for a single purpose – such as logging onto Amazon to buy products.

This report does not seek to provide a detailed and accurate technology description, but this appendix gives a summary of the main components in concept, for a citizen-led, distributed, and modular approach to digital identity.

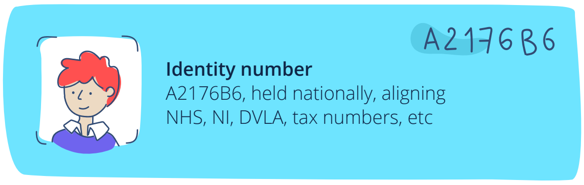
Identity Number

A digital identity is an information set that uniquely identifies an individual (see ISO 24760-1) for the purpose of IT processes. That processing could include authentication to systems and records.

For public services, it is often synonymous with a national identity – the unique citizen identifier for the purposes of digital and other non-digital government services. This unique identification can help to prevent fraud and error, as well as delivering more personalised and joined up services around individual needs and preferences.

In practice though, people legitimately have many digital personae – for family and friends, for government, for specific hobbies and interests, or on social media. But when it comes to transacting with government – receiving benefits, voting, passport application, paying tax – the ability to identify the single individual citizen is important.

> *"The legal and social effects of digital identity are complex and challenging. However, they are simply a consequence of the increasing use of computers, and the need to provide computers with information that can be used to identify external agents."*
>
> **Wikipedia**



Identity number
A2176B6, held nationally, aligning NHS, NI, DVLA, tax numbers, etc

Part of the challenge is that many people have multiple identities, and legitimately so. This may be to do with different names – a familiar name, a maiden name, or even a separate professional identity.

Authentication

System authentication is the process of establishing confidence in the digital identity of an individual for access to a system. It confirms that the identity works and that it is valid, reducing the risk of impersonation, fraud, or unintentional disclosure of personal data to a third party.

There are various methods of authentication used at different levels of sophistication to authenticate a user accessing systems and a variety of technologies (such as PKI, single sign-on, facial recognition, smart cards). Different methods may also be used for different systems, organisations, and purposes. These range from single to multifactor authentication, use of security tokens, challenge questions, and use of 3rd party certificating authorities.

A separation of 'digital identity' and 'authentication' can be helpful in allowing a single digital identity to be used across multiple systems with different authentication established, appropriate to the nature of the transaction being undertaken.

This can be helpful in public service transactions, where the individual citizen needs to be identified, but different methods and levels of authentication can be applied according to the nature of the access required.

Federated Identity

The idea of a federated identity is the mechanism that allows a digital identity to be shared across multiple distinct authentication and identity management systems.

An example would be the single sign-on within an organisation that allows an employee to access multiple systems through one authentication mechanism, where their security token (e.g., SAML - Security Assertion Markup Language) is passed across multiple IT systems or even organisations.

This is a critical component of joined up government, so multiple services can be linked together automatically around individual needs and preferences of the citizen to provide better services and public protection. It can also be used to tackle complex fraud in areas such as benefits.

There is a key element of trust; trust across the different systems and organisations that the federated identity is intact and valid, but also trust by the individual themselves in the way that their identity credentials are being shared across different public agencies.

This is best tackled by ensuring transparency in how federated identity is set up and how it works, especially across multiple public bodies, so that the citizen understands and can remain in control of how that federated identity works in practice, with simple 'opt in and opt out' mechanisms.

The ability to be able to pass authenticated credentials and a history of transactions between different agencies will depend on a variety of technologies, such as data matching. Time and care should be taken by public service organisations in linking relational services together in this way, to protect the individual as well as the credibility of the service.

Identity and access management

How individual organisations determine the nature of access management and definition of identity will vary.

Obvious examples are the way in which passwords are required to be defined, the regularity of password changes and the style of identity – e.g., in email formats. These are usually defined in clearly laid out organisation policies for security and data management which are mandated for individual employees.

It is these methods that, in practice, carry out the identification, authentication and access controls for individuals seeking to access systems and IT resources. Whilst individual organisations will take a unique approach to this, there are clearly grounds for national government to take a standardised approach. Only in this way for example can federated identity across multiple organisations and services function with confidence and safety.

App Stores

Many local authorities are developing 'App stores' for their citizens, as well as for visitors. This allows an individual to register and, with appropriate authentication, to link to a range of local authority-provided services.

Many of these in the past have been developed on a bespoke basis, using low code and no code developing tools, and in the absence of commonly agreed government standards.

In the future they should be based on commonly agreed open standards, with credentials being portable across different apps, organisations, services, and tiers of government, ensuring consistency in user experience and cyber protection wherever adopted.

Attributes

Attributes are things about the individual – that describe in increasing detail who that person is. A digital identity is not the same as personal attributes.

We use these all the time when proving identity in a non-digital situation. Things such as a last utility bill, bank account details, national insurance number, driving licence, mother's maiden name, mobile phone, education certificate, membership card – and many more – 'something you have, something you know'.

Attributes are used to initiate a digital identity, and then to link to a digital identity to provide the necessary level of authentication, so the credentials can be shared, or used to authenticate for services, shared as the user wants. Therefore, the design for UK digital identity solutions must be centred on the individual, since these attributes are the key to unlocking the digital identity for wider uses.

They need to be held separately and securely, and citizens need to know how to use them and to trust in their safety and security. Also, by being under the control of the individual, they can be updated and adapted as circumstances change.

Whilst a range of attributes are typically defined by the service providing organisation, the individual remains in control of their personal attributes, and can choose when and how they are shared alongside their digital identity, to access services and to conduct transactions.

Public service organisations providing security services can then check the personal attributes of the individual associated with the digital identity against the eligibility criteria to complete the interaction or transaction. Then, if the user agrees, the updated information can be shared across different services without having to repeat the process of authentication.

This means that an individual can associate an attribute with a digital identity for a period or a single purpose, but then remove it, holding it ready for next time. More importantly, it means less reliance on paper documents, and reduced risk of misuse, fraud, or error.

Appendix B: Case studies and examples

The following examples and case studies are included here to provide more background and illustrative detail on the relevant developments that have been referred to within the body of the report.

Case study: ID Cards

The UK public have a strong dislike of ID cards, and UK governments have never explained clearly to the public their potential value.

From the 1980s governments started to think about the value of reintroducing cards – to help with law and order, fraud reduction, immigration control, proof of age or entitlement, and service provision (such as library cards and bus passes).

Whilst the potential benefits grew in number as technologies advanced, so too did the concerns about a national identity card and its potential abuse. Police and security services were keen which compounded the public (and press) concerns. The UK public takes it as a basic right to have a private identity, and not to be required to carry a card with their photo on it or a number that can be traced and tracked.

From around 2005 the Labour government pushed hard to develop ID cards. The problem was that those considering cards did not (despite advice at the time) separate out the idea of a digital identity with the need to carry a card holding that ID. After all, people were happy to carry a driving licence or a passport, so what was the difference?

But the more information that an individual card held beyond the photo and a number, the more frequently that information would need to be updated. With that, came the greater the risk of personal information, often biometric, being lost, stolen or cloned. Dealing with data errors was also a worry, with a mistrust in how governments would deal with errors and whether minorities would be less well served.

There was also much debate about whether cards should be voluntary or compulsory. Whilst the idea of making cards optional would appeal to many, in practice the fear was that it would be unlikely that most people would be able to resist the pressure to have a card, partly because the implications of not carrying the card might be seen as having something to hide.

In 2008 the rollout of ID cards began, and in 2011 every British citizen aged 16 and over who made a passport application was automatically registered on the national database.

Despite this apparent progress, the overall system failed for two reasons:

- The public were not persuaded that they would benefit, rather than the government, or that the safeguards were sufficient
- No one had really worked out the cost, which transpired late on in the programme to be as much as £19 billion. The costs had accumulated because of complexity, administration, and maintenance.

On the cost model, it was even suggested that individual members of the public would be asked to pay for their own card – between £50 and £100, which was unlikely to be affordable.

Whilst there are clear benefits to having an identity card, and they are commonplace across western democracies, it should be operated on a distributed and non-mandated basis, with a national ID mechanism underpinning it.

This would allow local smart cards to be developed, using a national framework, but focusing on local public services designed for the benefit of residents and visitors.

Key points:

- Digital identity and identity cards are not the same. The way in which solutions should be developed by government must be modular and separating out the different components as described in this report

- A cost model needs to be established in advance, not just a business case, but the commercial basis on which sustainability will be maintained, and who will pay.
- Public trust should be at the forefront of development, gained through co-design, and transparency of purpose.
- Minimum data should be associated directly with a digital identity, with the citizen being given the choice of how the identity is used to connect to public services.

Case study: Government Gateway

This has become a widely recognised mechanism for UK citizens to register themselves online for government services. It has been in place now for 20 years and is commonly used to register for online services such as obtaining a driving license, filing tax returns or general queries with HMRC.

The original plan was that services on Government Gateway would be replaced by GOV.UK Verify by 2019, but problems with Verify have made this untenable. HMRC are developing their own service which allows users to sign in using the existing government gateway user ID.

Whilst the Government Gateway system is somewhat clunky to set up, it functions broadly well, although it has both technical and business limitations for ongoing development. The challenge for UK government lies in the numerous different approaches that are now being taken to digital identity and authentication for access to public services.

Case study: Greater Manchester Authority

GM Identity (GMID) is Greater Manchester's Identity and Access Management (IAM) service and is a collaboration between the Greater Manchester Combined Authority (GMCA), the Greater Manchester Health and Social Care Partnership (GMHSCP) and Shaping Cloud, a technology innovator based in Manchester.

GMID is based on current standards and developments in digital identity and aims to build a new digital product that enables seamless access and sharing of apps and data across organisational boundaries.

It was launched in 2020 as a key part of the wider Greater Manchester Digital Platform to deliver robust and secure data sharing and application development. GMID is supporting ambitions within Greater Manchester's Digital Blueprint - to ensure that everyone in the region can benefit from the opportunity digital brings and offer digital access to public services that is joined up, user friendly and makes sense.

With a growing need to collaborate regionally and to deliver joined up public services, a move away from on-premise, single sign-on solutions was required. Faster deployment and the ability to adapt quickly to changing legislative and resource demands pointed towards a GM-wide IAM solution.

The GMID ambition is to rationalise resources, share assets, control authorisation and authentication and lessen the 'red tape' for public service organisations, and for citizens accessing those services. Removing the current plethora of systems and login credentials would also make it easier for staff to move between organisations and to work collaboratively.

GM Identity technology:

GM Identity brings together Microsoft's Identity stack including on premise Active Directory instances, AAD, AAD B2B, and AAD B2C. It also incorporates the latest identity frameworks, standards, and protocols, as well as automated workflows to enable non-technical staff to manage access to resources.

GM Identity also incorporates NHS standards, NHS Mail, and NHS Login and is one of the first non-NHS apps to be authorised by the NHS to do so. This creates a flexible and secure federated identity, authentication and authorisation service for NHS and government organisations.

Identity credentials and user permissions follow users across the network of apps and tooling, reducing account creation and maintenance tasks across all administrative touchpoints.

Azure cloud and best practise in authentication, together bridge the gap between currently available Microsoft services and bespoke 'line of business' systems. It works with multiple identification providers and trust vectors, to share central role or attribute data. This allows a consistent single sign on experience and flexible authentication methods, integrating NHS Login and NHS-compliant identity verification for patient access to data and systems.

Today, GMID is being used in applications to reduce smoking in pregnancy, digitise child development plans, and facilitate interactions with various stakeholders regarding school age children's development requirements. Information can be shared between the public, health care professionals and local authority teams, safe in the knowledge the data is secure and being accessed by appropriate parties.

Having created a system that can handle both small and large-scale implementations, the future vision is to build deeper within and across organisations. This includes plans to support Greater Manchester's ambitions to tackle homelessness and rough sleeping, facilitate education funding, aid hospital discharges and support patients' treatment journeys through complex ecosystems, amongst others. There are also plans to support internal business operations:

- Include further identity providers to widen citizen and non-GM staff access.
- Enable the easier movement of staff between organisations.
- Facilitate the access of network-based devices and Wi-Fi.
- Lessen the administrative burden of 'joiners, movers and leavers' with integration into HR systems.
- Widen the user management interface capability to allow developers to manage their GMID configurations and administer users.

Case study: GOV.UK Verify (Verify)

The Verify programme started in 2011 and had reportedly cost a total of £220 million before being closed ten years later in 2021. Whether or not all or some of the previous system components will be reused is not yet known, but the next version of Verify is apparently already underway. The lessons from the failed Verify programme need to be learned (whether for its replacement, or any alternative programme of a similar nature).

Digital projects that are unsuccessful usually have problems early on in their development – they do not all go wrong at the end. After more than 20 reviews of Verify over a five-year period, with many issues being reported, it is surprising that the project was not terminated earlier.

A broad timeline of the issues can be found in figure 10.

Figure 10. Timeline of GOV.UK Verify issues

2011

- The programme is announced as the Identity Assurance Programme (IDAP)
- A launch date of 2012 is agreed

2013

- Piloting of local government services begins over the next few years, particularly bus passes and blue badge, as well as disabled parking permits

2014

- The programme formally relaunched to embrace further government services

2015

- The business case is agreed, and ambitions published:
- To become the standard digital identity scheme for accessing online public services, and to be extended for use in the private sector
- "90% of people can verify their identity online with a 90% success rate by April 2016"
- To protect the public sector digital services from cyber threats including identity fraud and malicious activity

2016

- Verify goes live with a launch in May 2016 four years later than originally planned

2017

- The government announces a target of 25 million Verify users by 2020 (800,000 per month)

2018

- £130m has been spent on the programme
- The Cabinet office project authority recommend that Verify should be terminated because of dwindling support
- Cabinet Office Minister Oliver Dowden agrees one more funding round to transition to a private sector-led model
- The Verify business case is re-written
- Contracts are signed with five identity providers – Barclays, Digidentity, Experian, Post Office, and Secure Identity
- Royal Mail and Citizen Safe pull out
- DCMS take over policy responsibility for digital identity, planning to create an ecosystem of providers, based on government backed standards for interoperability of digital identities
- HMRC decides to develop its own version of the existing Government Gateway solution, and NHS England planned to do the same, stating that Verify was not secure enough. The Scottish Government equally pressed ahead with its own digital identity plans
- DWP create an additional identity system to support Universal Credit after finding that more than 60% of benefit claimants couldn't register on Verify

Figure 11. Timeline of GOV.UK Verify issues (continued)

2019

- Verify project costs rise to £155m
- The Civil Service CEO John Manzoni describes the original Verify business case as containing "hopelessly optimistic projections" when challenged by the public accounts committee (PAC)
- Lisa Barrett is appointed as director of digital identity at the GDS to oversee Verify

2020

- Lisa Barrett leaves the government programme after little over a year
- £175 million has been spent on the programme to date
- Three more private sector identity providers leave the programme, leaving only the Post Office and Digidentity
- TechUK adds its voice to the criticism
- A Digital Identity Unit (DIU) in DCMS combines resources from the GDS Verify team
- A planned trial involving the use of passport data in the private sector is delayed
- The NAO release a report that criticises the programme and decisions are taken
- The PAC concludes that Verify was failing its users, had not delivered value for money and its leaders have not accepted proper accountability for the troubled programme
- The Infrastructure and Projects Authority which oversees major government programmes, gives Verify a 'red' rating – meaning it is considered unachievable
- Only six million Verify accounts have been created, with 22 services including Universal Credit, although still just over 50% of people trying to authenticate themselves fail to be able to do so

2021

- Around £220 million has been spent on the programme to date
- It is accepted that Verify has not succeeded and must be terminated (it will run until 2023)
- The Cabinet Office Minister Julia Lopez confirms that Verify had "over-elaborate expectations, trajectory and cost"
- The Cabinet Office begins work on a new common digital identity system, to be used across central government
- DCMS begins its wider consultation on digital identity policy across the wider economy, publishing its alpha version of its digital identity trust framework

Case study: Coronavirus contact sharing

Although not done well (by most measures) it was a remarkable achievement to roll out a universal contact tracing system into the UK culture so quickly. It was only (mostly) accepted because of the seriousness of the impact of the virus, and that support will inevitably reduce as the impact of the virus reduces.

However, it demonstrates what is possible, and the degree of public acceptance when they need it. There were useful learning points from the development in terms of digital identity development for the future:

- 'Build your own' is not easy for governments, however well-intended. Eventually this was recognised in the way in which the track and trace system was being rolled out, and the importance of being able to integrate with the main types of smart phones
- Many people do not use it because of uncertainty in how data is used, and this remains a problem. This is partly about trust, but it is also about being able to answer the question: "what's in it for me?"
- Data was not shared with local authorities at an early stage, limiting the rollout success. Indeed, many in local government argue that they were best placed to make a success of the track and trace system, especially in contact chasing.

It is quite likely that digital vaccine passports will play an important part in the future of digital identity development. Driven by the desire for freedom of movement, including for holiday and work, the idea is gaining traction with the public. This is despite the concept being worrying for some people who will be suspicious of credentials being used to restrict their activity or for other purposes.

Vaccine passes will therefore need to be voluntary under the control of the user, with strong protections for personal data and privacy.

Importantly, a growing lack of support for contact tracing in what was hoped to be the latter stages of the pandemic resulted in many cities switching off the app, which undermined its effectiveness.

Case study: Digital Identity Scotland (DIS)

The Scottish Government, in parallel with the UK initiatives described in this report, is pressing ahead with its own identity programme, Digital Identity Scotland (DIS).

The main aim of the programme is to improve citizen access to public services by providing a safe, reusable, and easy way for them to prove who they are or that they are eligible for a public service. This seeks also to bring consistency across multiple public service providers, reducing the amount of personal information that public organisations need to store and protect.

Differing from the GDS digital identity and SSO programme, the Scottish project starts explicitly with local user cases in a collaborative endeavour with local government. In other words, looking at public service requirements from a holistic, user perspective.

The design is based on delivery of a digital identity 'attribute store/personal locker' based model and will be voluntary for people to use. It will offer those seeking to access public services choice and control about whether to store their personal information and what they share with individual public service providers.

Central to the design and addressing one of the issues which compromised the Verify programme, DIS has a specific focus on those people who are unable or unwilling to access services online, by offering alternatives and mediated access where required.

Case study: Government Digital Service

As stated in the GDS strategy 2021-2024, GDS seeks to:

> *"Build a simple, joined-up and personalised experience of government for everyone. We will develop services that just work for the user, however complex the underlying systems."*

The 'Mission 3' statement within the strategy relates to the development of digital identity solutions, recognising the need, the current problems and principles for design and development. GDS recognises that fragmentation of identity approaches across the UK public sector has led to higher costs, inconvenience for citizens and greater risk of digital fraud.

The challenge lies in fulfilling these principles. As GDS focuses on central government high-volume transactions to initiate the its replacement, it leaves the more complex relational services of local government and health until later, thus compromising the viability.

The next iteration of the 'Verify' programme, now being terminated after ten years of only partial delivery, at a cost of over £220m. This new solution from GDS will reuse elements of the Verify system and is being developed on a rapid and iterative basis. The risks of a fast and immediate development lie in:

1. Not having the time and space to truly learn lessons from the failed programme
2. Reusing elements that would potentially be best replaced or re-designed
3. Repeating a centrally-driven design methodology
4. Failing to take sufficient time to understand and to test 'use cases' in the areas where Verify failed.

One of the GDS design principles advises starting with the user experience, and it is looking likely that this will be infeasible.

Mission 3: A simple digital identity solution that works for everyone

Most government services' existing login and digital identity solutions have been designed, developed and operated in departmental silos, with a focus only on meeting each department's needs. For users, this is a confusing and frustrating picture; for government, this is expensive and leaves the door open for fraud.

We will build on what we have learned from GOV.UK Verify and create a new way for users to sign-on to services from any department, and confirm their identity.

The work will follow some basic principles:

- The new services will be built in partnership with other government departments.
- The identity checking service needs to work for everyone in the country, regardless of their socio-economic situation. For example, someone who is a prison leaver and may not have a fixed location, or someone with an address but has a passport that has expired.
- We will design-in simplicity and relentlessly test with users.
- Existing services will only be integrated, absorbed or turned off when the new service has been tested thoroughly, and everyone is happy that it works as it needs to.
- Users will have full control over their data from their GOV.UK account, and the connected data we hold.

For example, given the transitory nature of significant groups of the UK population, an important requirement for local government is that, if the proof of identity has been secured by a local authority, that identity proof should be portable, if agreed by the citizen. This means that it could be reused to access other local authority or central government services. This fundamental principle was not understood or adopted in the first iteration of Verify.

The DCMS approach in establishing common components for digital identity, as described in this report, would help to address this issue, and has been requested as the preferred approach for the last two decades by organisations such as Socitm and its Local CIO Council (LCIOC).

Most government services (and local councils) have incompatible digital identity solutions designed, developed, and operated in silos for specific purposes, because a single GDS-lead solution has not been available (or worked).

A modular and componentised approach, based on recognised and agreed pan-public sector standards, would allow a distributed approach to development based on common standards and reusable digital components in contrast to the repeated failure of centralised design models.

This would create the flexibility in design that could be adopted by local public services such as health and local government, opening the opportunity for place-based provision of individually focused and integrated services that address the personal circumstances of citizens.

Arguably, therefore, the solution is not to build another system. Rather, it is to start with a blueprint of standards, design models and digital components, which can be shared. Development can then be federated and accredited across the public sector, with confidence in interoperability. This will also tackle the problem that there are just too many disparate and incompatible digital identity systems.

The onus should be on the owners of those systems to ensure that, in an agreed timescale, they adapt their solutions or replace them to reflect the standards-led approach. That should include all the recognised existing methods, including those from HMRC, DWP and the NHS, as well as local government's citizen-facing identity solutions.

This might mean that there is a place for GDS to work with government departments and other agencies in developing user case solutions in accordance with the agreed standards, but development would only be when specifically required. Whilst the scope and design of Verify's replacement are not assessed by this report, it is hoped that the wider recommendations made here will be included.

Case study: DCMS

DCMS have determined that they will develop a set of rules in a 'trust framework' for digital governance that can be used by public and private sectors alike. Because of its importance, it is included in the body of the report.

DCMS are not developing the digital identity or the authentication access methods themselves, but rather specifying how things should be done and how organisations can be accredited to adopt them.

They are committed to developing a central governance function, removing, and adjusting legislative and regulatory blockers where required.

> *"It is not my department's intention to provide any new ready-made solutions or actual products – we will be relying on the creative and innovative drive industry to build the services to meet the needs of consumers from all walks of life. The trust framework is intended to set out the rules for the services, to provide the playing field on which businesses can operate."*
>
> **Matt Warman MP, Minister for Digital Infrastructure, DCMS**

This approach could potentially work across the public sector, creating the appropriate trust framework that is common to public and private sectors.

Indeed, the DCMS consultation document indicates that the GDS will be working with government departments to develop across-government single sign-on identity solution which would be based on this, with interoperability of identities and associated attributes between sectors in the longer term.

DCMS is working across industry, civil society and government departments, as well as the wider public and third sectors. It is also looking at international interoperability although Norway, referenced in this report, is not included. The challenge will lie in the ability to deliver against this vision, reconciling the demands of the public sector in diverse places.

Case study: the NHS app

The NHS app allows users to access a range of NHS services on their smartphone or tablet. It was launched in 2018 and offers services including symptom checking and triage, appointment booking, repeat prescription ordering, access to patient records, national data opt-out, and organ donation preference.

Since September 2019, the number of registered NHS app users has risen from 91,000 to over 6 million, largely because it offers potential proof of vaccination (although the NHS app is separate from the NHS 'Track and Trace' Covid-19 app).

It connects a unique digital identity through authentication to a range of nationally held and distributed health data about an individual. The intention is to link 55 million GP patients' data, and Greater Manchester Authority is already considering this mechanism as an authenticated access and digital identity for a wider range of local public services.

With a combination of a successful launch and public trust, this app could in theory be generalised as a citizen digital identity mechanism. But this is unlikely to be possible if multiple different government departments, agencies and local authorities remain focused on individual and bespoke developments for their own specific service needs.

If this generalisation were to prove possible then it will be important to ensure:

- That the NHS app is not developed in isolation and that other public service organisations can use the same digital components in due course.
- It becomes the defacto basis for common digital identity standards for public services – technical and policy frameworks to support interoperability.
- The commercial and public service ambitions are clearly laid out, following the principles promoted elsewhere in this report (e.g. 'citizen in control', standards and standardisation, modulatory of design, etc).
- If any data held within the app is to be shared between public bodies, research organisations, charities, or the private sector then this can only happen with the specific agreement of the individual citizen.

A number of national NHS digital programmes have failed over the years - it is arguably the worst track record of any public service (NPfIT and Care.Data being the most visible).

Without the support of professionals, the press, public and politicians, digitisation of health services will never be successful however laudable and well-intended, and the early success of the NHS app could easily be undermined.

Case study: NHS Digital Staff Passport

The NHS is currently working on developing a Digital Staff Passport, given many staff move between organisations in their jobs and as their careers develop. Much time is lost reprovisioning digital identity for access onto local systems

This will allow NHS professionals to move between organisations, taking their unique identity with them. It will make systems more interoperable, with verifiable data contained in a 'digital wallet'.

The intention is that this could in future also include social care staff and volunteers, and even potentially citizens.

About this report

Author
Jos Creese – Independent digital consultant, researcher and analyst

Editor
Martin Ferguson – Director of policy and research
David Ogden – Communications manager

Designers
Magdalena Werner – Senior creative designer
Benjamin Hughes – Graphic designer

Special thanks to:

William Barker, Socitm

Russ Charlesworth, Socitm Advisory

Alexandra Murphy, Socitm

Ben Cheetham, MHCLG Local Digital

Geoff Connell, Norfolk County Council

Paul Davidson, iStand

Tom Denman, LGA

Sheldon Ferguson, MHCLG Local Digital

Phil Swan, iNetwork

Members of the Socitm Local CIO Council

Have your say

We always welcome feedback and discussion on the contents of our publications.

Martin Ferguson
Director of policy and research
martin.ferguson@socitm.net

Nadira Hussain
Director of leadership development and research
nadira.hussain@socitm.net

Get in touch

Website: www.socitm.net
Email: inform@socitm.net
Tel: 01604 709456

Join the conversation... @Socitm | Socitm