

Managing digital identity

National Audit Office Report

To: All Chief Executives, Main Contacts and APSE Contacts

1 Executive summary

The National Audit Office (NAO) recently published its *Managing digital identity* report, examining the development of digital identity in the UK and drawing on previous UK experience and international examples to identify lessons for government. The report was largely completed before the [UK Government announced in July 2026](#) that it would not proceed with its proposals for a single government-issued digital identity. However, the NAO believes that the underlying challenge of enabling people to prove who they are and demonstrate their entitlement to public services securely and conveniently remains relevant.

For local authorities, the report provides useful lessons as councils continue to digitise services and look for ways to make interactions with residents simpler and more efficient. The NAO emphasises that digital identity is not a single product or technology, but an ecosystem involving identity services, credentials, standards, data, technology providers and government arrangements. It highlights the particular difficulties created by fragmented public services, legacy systems, inconsistent data and different approaches to identifying individuals.

The NAO concludes that successful digital identity depends on clearly defined objectives, realistic expectations around cost and timescales, effective integration between systems, appropriate governance and public trust. These lessons are directly relevant to councils considering digital identity as part of wider digital transformation, particularly where they are seeking to join up services, reduce duplication and provide residents with more seamless ways to access services.

[Click here](#) to read the full report.

2 Overview

Digital identity is becoming an increasingly important part of how people access public services. Put simply, it allows someone to prove who they are, or demonstrate that they are entitled to a particular service or benefit, without necessarily having to do this in person or provide the same information

repeatedly. It can involve a range of technologies and approaches, from government-issued credentials and identity verification services to digital wallets and credentials held on mobile phones.

The National Audit Office (NAO) describes digital identity as an ecosystem rather than a single technology or product. This ecosystem includes government and private sector providers, legislation, standards, identity credentials, verification services and the systems used by organisations to manage information about individuals. The UK already has a range of legislation, standards and digital identity services that provide a foundation for further development, but the NAO identifies significant challenges arising from the fragmented nature of public services and long-standing differences between systems, as this can make it more difficult to connect information about the same person across different services.

This is an important point for local government. A resident may already have information held by a council across several different services, for example in relation to council tax, housing, benefits or other local services. Simply giving that resident one way to prove their identity does not necessarily mean that the council's different systems will be able to recognise and connect that person correctly. Improving the way existing systems and information work together can therefore be just as important as the digital identity itself.

The report identifies four broad areas that need to be considered when developing digital identity:

- Clarity of design and objectives: organisations should establish what problem digital identity is intended to solve, and understand their existing business processes, data requirements and integration challenges before developing technology.
- Users and trust: digital identity systems are more likely to succeed where people understand them, trust them and see a clear practical benefit from using them.
- Data and alignment: establishing a verified identity is only one part of the challenge. Organisations also need to ensure that the identity can be connected to the correct record and information across different systems.
- Enablers of delivery: successful implementation requires realistic assumptions about costs and timescales, alongside clear decisions about funding, ownership, accountability and the role of the private sector.

2.1 Lessons from previous digital identity programmes

The NAO draws on previous experience in the UK and internationally to identify some of the challenges involved in introducing digital identity on a large scale. One of its main messages is that these projects can be more complicated and take longer than originally expected, particularly where they involve bringing together existing systems and organisations.

The report suggests that organisations should be clear about what they are trying to achieve before

deciding what technology to introduce. There is a risk that a new system can be developed because the technology is available, without first establishing whether it will actually improve the service being provided. The NAO therefore places importance on understanding the purpose of a digital identity system and the problems it is intended to address before deciding how it should work.

Previous experience also shows that the benefits of digital identity may not appear immediately. Introducing a new system can involve changes to existing services, staff processes and information, as well as technical work to connect different systems. These changes can make projects more difficult and expensive than initially anticipated.

The NAO highlights the importance of understanding existing systems and information before attempting to introduce a new digital identity approach. Where organisations have older systems or information that is incomplete or inconsistent, these issues may need to be addressed before the full benefits of digital identity can be achieved. This means that a digital identity project can sometimes involve wider changes to how an organisation manages information and delivers services.

The report also notes that the UK Government's efforts to date have focused heavily on enabling people to reuse a verified identity across online services. However, this addresses only one part of the wider identity challenge. Government must also be able to identify the correct record belonging to that person within each individual service.

2.2 Making digital identity useful for residents

The NAO's research suggests that people are more likely to use digital identity when they can see a clear benefit from doing so. In countries where digital identity has become widely used, this has generally been supported by services that people find useful and easy to access.

Trust is also important. People need to understand what a digital identity is being used for, what information is being collected and how their information will be protected. If residents are unsure about these issues, they may be less willing to use digital services.

The report suggests that simply making a digital identity available does not guarantee that people will use it. People need to see that it makes accessing a service easier, quicker or more convenient than existing options. This is particularly important where people are being asked to provide personal information or complete identity checks, as they need to have confidence that there is a good reason for doing so.

This is particularly relevant for local authorities because councils provide services to communities with very different levels of digital access and confidence. Digital identity may make some services quicker and more convenient, but not everyone will have the same ability or willingness to use digital services.

The NAO therefore highlights the importance of considering the experience of users when developing digital identity, rather than focusing solely on the technology itself. Clear information

and support can help people understand how a system works and why they are being asked to use it.

2.3 The changing digital identity landscape

The report also considers how digital identity is developing. One emerging area is the use of mobile phones and digital wallets, which can allow people to keep digital credentials or other forms of evidence on their devices. Other countries are developing approaches that allow identity information or credentials to be reused across different services.

These developments could make it easier for people to prove information about themselves without having to repeat the same process each time they access a service. For example, a person could potentially use a digital credential stored on their phone to demonstrate information about themselves when accessing different services.

However, the development of these technologies also means that different systems need to be able to recognise and work with the same information. The NAO highlights the growing importance of common standards and arrangements that allow different services to work together. Without this, people could still find themselves having to use several different systems despite have digital credentials available.

The report does not suggest that there is one approach that all governments or public bodies should adopt. Instead, it highlights the need for organisations to consider what approach is most appropriate for their own circumstances and the services they provide. This is particularly relevant as technology and people's expectations around accessing services continue to change.

2.4 Costs, responsibility and delivery

The NAO also highlights the need for realistic expectations around the cost and timescale of digital identity projects. The technology itself is only one part of the work involved. Connecting it to existing systems, changing the way services operate, improving information, training staff and maintaining the system can all require additional resources.

The report suggests that organisations need to consider these wider requirements when planning digital identity projects rather than focusing only on the initial cost of developing or purchasing a system. Projects also need clear responsibility and accountability, so that it is understood who is responsible for delivering the system and dealing with problems when they arise.

The NAO also recognises the significant role already played by private companies in providing digital identity services. This raises questions about how much digital identity infrastructure should be provided directly by government and how much could be provided by private organisations within appropriate rules and safeguards.

For local authorities, the wider lesson is that digital identity is unlikely to work effectively as a standalone project. It needs to fit with existing services, systems and information, while also

providing a clear benefit to the people using those services. Councils will therefore need to consider the wider practical and financial implications before introducing new digital identity arrangements.

3 Implications for local authorities

Although the NAO report does not specifically focus on local government, its findings are relevant to councils as they continue to develop digital services. The report suggests that digital identity should not be viewed simply as a new piece of technology. Councils considering digital identity will first need to be clear about what they are trying to achieve and whether it will make services easier for residents or reduce administrative work for staff.

One of the main issues highlighted by the NAO is that proving who someone is only accounts for part of the challenge. The information then needs to be linked to the correct record held by the organisation providing the service. For councils, this could be particularly relevant where different services use separate systems or hold information in different ways. Introducing a new digital identity system may therefore require changes to existing systems and information, rather than simply providing residents with a new way to log in.

This could also be relevant where councils work with other public services. Residents may need to provide similar information when accessing council services alongside services provided by other public bodies. There may be opportunities to make these processes simpler, but sharing information between organisations also raises questions around privacy, security and who is responsible for the information being used.

The experience of residents will also be important. The NAO highlights that people are more likely to use digital identity where they see a clear benefit from doing so and where they have confidence that their information is being handled appropriately. Councils will therefore need to consider how any new digital identity arrangements are explained to residents and whether people have other ways of accessing services if they cannot or do not want to use digital options.

There are also likely to be financial and organisational considerations. The cost of introducing digital identity is unlikely to be limited to the technology itself. Councils may also need to consider the work involved in connecting existing systems, improving information, training staff and maintaining new arrangements. Given the financial pressures facing local government, it will be important that councils have a realistic understanding of these costs and the benefits that are expected in return.

Overall, the NAO report suggests that digital identity is most likely to be useful when it forms part of wider improvements to how services are delivered. For councils, this means considering digital identity alongside existing systems, the quality of information held by the council, the needs of residents and the resources available to deliver and maintain changes.

4 APSE Comment

The NAO's report provided a useful overview of some of the opportunities and challenges associated with digital identity. While the report is not specifically about local government, its findings are relevant to councils as they continue to move more services online and look for ways to make services easier for residents to access.

One of the most useful points for local authorities is that digital identity is about more than simply providing residents with a new way to log into services. If councils have different systems holding information about the same residents, introducing a common way of proving identity will not necessarily resolve the problems between those systems. The NAO's discussion of existing systems and information therefore provides a useful reminder that wider improvements may be needed alongside any investment in digital identity.

There are clear potential benefits for councils. A trusted way for residents to prove their identity could make it easier to access several services and reduce the need to repeatedly provide the same information. It could also reduce some administrative work for staff. However, these benefits will depend on digital identity working effectively with the services and systems that councils already use.

The experience of residents also needs to remain central to any changes. Digital services can make it easier for many people to access council services, but not everyone will have the same level of digital access or confidence. Councils will therefore need to consider how digital identity fits alongside other ways of accessing services and make sure that people who need additional support are not left behind.

The report's findings around cost and implementation are also relevant at a time when councils are under considerable financial pressure. Digital identity may offer opportunities to improve efficiency, but councils will need to consider the wider costs involved, including connecting systems, maintaining technology and supporting staff and residents. The expected benefits therefore need to be realistic and linked to a clear improvement in the service being provided.

Overall, the NAO report highlights that successful digital identity depends on more than the technology itself. For local authorities, the main consideration is likely to be how any digital identity approach fits with existing services, systems and the needs of local residents. Used appropriately, it could form part of wider efforts to make council services simpler and more accessible, but it should not be seen as a solution to wider digital or organisational problems on its own.

5 How can APSE help?

APSE provides opportunities for local authorities to share experiences and approaches to service transformation through its networks. The Social Value, Procurement and Commercialisation Network provides a forum for councils to discuss new approaches to service delivery, efficiency and the use of technology across local government. As well as discussions within the other service

specific networks including Construction, Housing and Building Maintenance around the use of technology and service transformation. Network meetings are free to attend for APSE members. Previous presentations are available online [here](#) and upcoming meetings are listed [here](#).

APSE Southern's Digital Futures Forum is also taking place on Thursday 24 September, this forum will look at AI solutions and the use of technology to improve efficiencies. For more information on this forum please [click here](#).

David Hinds,
Research and Information Officer
dhinds@apse.org.uk

Louise Melville,
Policy Lead (Scotland)
lmelville@apse.org.uk

Sign up for APSE membership to enjoy a whole range of benefits

APSE member authorities have access to a range of membership resources to assist in delivering council services. This includes our regular network meetings, specifically designed to bring together elected members, directors, managers and heads of service, together with trade union representatives to discuss service specific issues, innovation and new ways of delivering continuous improvement. The networks are an excellent forum for sharing ideas and discussing topical service issues with colleagues from other councils throughout the UK.

Networks are a free service included as part of your authority's membership of APSE and all in-person networks end with an informal lunch to facilitate networking with peers in other councils. If you do not currently receive details about APSE Network meetings and would like to be added to our list of contacts for your service area, please email enquiries@apse.org.uk.

Our national networks include:-

- FM and Building Cleaning
- Catering (School Meals)
- Cemeteries and Crematoria
- Highways and Street Lighting
- Housing, Construction and Building Maintenance
- Social Value, Procurement and Commercialisation Network
- Parks, Horticulture and Grounds Maintenance
- Renewables and Climate Change
- Roads, Highways and Street Lighting
- Sports and Leisure Management
- Vehicle Maintenance and Transport
- Veterans and Military Champions Network
- Local Government Reorganisation Network
- Waste Management, Recycling and Street Cleansing

Visit www.apse.org.uk for more details.



INVESTORS IN PEOPLE™
We invest in people Gold

Association for Public Service Excellence
3rd floor,
Trafford House,
Chester Road, Manchester M32 0RS.
telephone: 0161 772 1810
web: www.apse.org.uk

NEW MUNICIPALISM
Delivering for local people and local economies