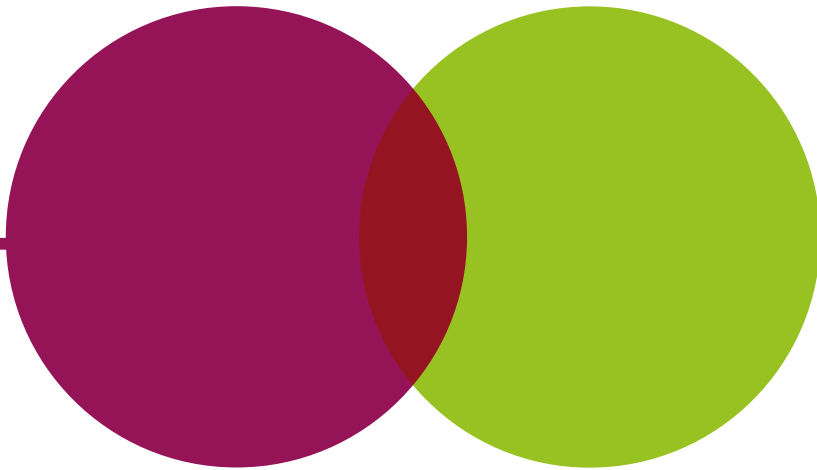




National Audit Office



INSIGHT

Managing digital identity

Department for Digital, Culture, Media & Sport

SESSION 2026-27
2 SEPTEMBER 2026
HC 586

Summary

Introduction

- 1** Identity underpins access to public services, the prevention of fraud and error, and the safe use of information across organisations. As services become increasingly digital, decisions about how identity is established, verified and governed have significant implications for service delivery, privacy, trust, security and the efficient use of public resources.
- 2** In July 2026, the government announced that it would not proceed with proposals for a government-issued digital identity. However, questions about how individuals verify their identity and prove eligibility for services remain important. A range of digital identity-related services, credentials, standards and governance arrangements already exist across government and the private sector. Understanding how these arrangements operate, and the lessons from UK initiatives and international experience, remains relevant to future decisions about identity verification, authentication and access to public services.
- 3** Proof of identity in the UK still relies largely on physical documents such as passports and driving licences, often supported by bank statements and utility bills. Reliance on physical items can make it difficult for people to prove who they are, something about themselves or their entitlement to something in digital settings. A well-designed digital identity can achieve this. It can also limit unnecessary data sharing by supporting selective disclosure, for example by enabling someone to prove they are over 18 without having to reveal their actual date of birth.
- 4** Many people already hold one or more forms of digital identity for various purposes. It is not a single product. Rather it is an ecosystem of services and technologies provided by the government, the private sector, or both. Many identity services in the UK are provided by private companies within government standards, and use is often voluntary. Convenience, saving time, privacy and security are the most important factors influencing whether people use digital identity services.
- 5** Designing how multiple digital identity components fit together, including how data is accessed, verified and reused across services, is complex. The current landscape is fragmented and the question is how coherent the overall system should be. A more coordinated approach enables governments to have clearer choices and a better understanding of the benefits, costs and trade-offs of different delivery models.

6 This report draws on the NAO's previous work on digital transformation, data and government's previous work on identity, together with evidence from international audit bodies. It examines the scope and purpose of digital identity, the UK landscape including the roles of the government and the private sector, international experiences and emerging developments, and it identifies the characteristics associated with successful approaches.

7 The report provides insights from UK and international experience to help inform any future consideration of digital identity, including the trade-offs that can affect cost, complexity and value for money. It does not examine or evaluate the performance of any specific programmes or organisations.

Key findings: insights for government

Clarity of design and objectives

8 Implementing digital identity at scale across fragmented public services is a complex integration challenge requiring long timescales. Digital identity is an ecosystem of interdependent services, components and technologies. Determining how they should fit together requires clear up-front thinking, planning and sequencing of delivery. The more purposes a digital identity system is expected to serve, the more complex it becomes to design and deliver. This means that early decisions about design and data integration are critical. Experience suggests that any future initiative involving digital identity would benefit from a clear plan and roadmap. Without these, there is a risk that disconnected solutions develop which fail to address the end-to-end challenge of connecting citizens' data and services. As a result, investment may not deliver the intended benefits or represent value for money (paragraphs 1.2 to 1.7, 1.18 and 1.19).

9 International experience shows that there is no single model for digital identity. Countries have adopted different approaches to suit their institutional and social contexts. For example, Sweden provides digital identity via private companies, especially banks. In Denmark, the government sets standards and works with the banking sector, which provides the underlying technology. Countries such as India and Singapore use state-issued identity. Furthermore, some countries have introduced a single shared identifier to identify a person across different government services, while others have deliberately chosen not to do so. For example, India's Aadhaar single identifier system initially suffered from a variety of security and privacy issues, leading to a more secure approach being adopted. These differences illustrate that governments need to make explicit choices about their preferred approach and delivery model (paragraphs 1.12, 1.13, 1.22 and 4.3).

10 A digital identity is less likely to deliver its intended benefits where technology is built before the objectives, business processes, data constraints and integration challenges are clearly understood and addressed. We have previously reported on the difficulties that the government has experienced in delivering complex digital change in the face of persistent structural challenges. This has especially been the case where technology-enabled business change programmes focused on trying to build a technical solution quickly before thinking through the business and integration issues. For example, GOV.UK Verify did not resolve end-to-end identity processes across government, meaning it was not adopted at scale and did not achieve its intended outcomes. Experience from the UK and internationally indicates that proposed benefits are more likely to be achieved where government sets out its intended outcomes and explains how its chosen approach offers best overall value for money, including the options considered, costs, risks, required changes to processes and any new dependencies created (paragraphs 4.3 to 4.7 and 4.13 to 4.18).

Users and trust

11 Outside of countries with a history of mandatory identity systems, successful digital identity relies on people finding it useful and wanting to use it. Take-up is linked to whether systems provide clear, practical benefits in everyday use. Convenience, time savings and the ability to reuse identity across multiple services encourage adoption. Concerns about privacy, security and data can act as barriers. Where digital identity services are not perceived as useful, or offer limited advantage over existing processes, uptake has tended to be low. Conversely, systems that are integrated into high-value services and reduce friction for users are more likely to achieve widespread use (paragraphs 1.14, 1.15, 2.17, 2.18, 4.8 and 4.9).

12 The UK already has legislation, standards and digital identity services that provide a foundation to build on. A range of public and private sector digital identity services exist. But proving identity is complex and inconsistent across services. For example, digital identity from certified private sector providers is not currently acceptable as voter identification at polling stations. Greater consistency, clearer rules on where approved digital identities can be used, and improved usability are important factors in encouraging adoption. Without these, fragmentation is likely to persist, limiting uptake and reducing the benefits of digital identity across services (paragraphs 2.4 to 2.13, 2.23 to 2.25, 4.2 and 4.12).

13 Trust and adoption will depend on how clearly governments explain the different aspects of digital identity. Concepts about data access, privacy, authentication and verification can be complex and are not well understood by most people. Unclear or inconsistent communication will undermine trust and adoption, even where implementation may be technically sound. Where governments seek to expand the use of digital identity, experience suggests they need to explain clearly what digital identity does and does not do, how data will be protected and how individuals will be able to exercise choice and seek redress where needed. Experience also suggests the importance of being realistic about what can be delivered and over what timescales (paragraphs 4.12 and 4.19 to 4.24).

Data and alignment

14 The government's efforts to date have mainly focused on allowing people to reuse a verified identity across its online services, but this addresses only one aspect of identity reuse. Allowing someone to use the same identity to log in to different services does not automatically connect the underlying data across those services. After a person's identity is verified, government must still match them to the correct records in each different system. This remains a challenge because of the long-standing issues we have previously identified with government's fragmented and poor-quality data (paragraphs 1.9, 1.10 and 1.17).¹

15 Linking records about the same person across different systems and organisations is a separate challenge. Legacy systems which use inconsistent data standards and have multiple ways of representing the same person compound the problem. Individuals can appear differently across different systems, making it hard to link data and limiting the ability and effectiveness of joining up data across different services. Unless addressed, these issues would be a practical constraint on what a digital identity could achieve (paragraphs 1.18 to 1.22).

16 Phone-based digital identity is a more recent development that is reshaping user expectations and how systems work together. Regardless of their history of identity schemes, many countries are exploring or implementing phone-based digital identity. Digital wallets are integral to these newer forms of digital identity and provide a secure way to store and validate digital versions of documents (such as a driving licence) on a phone. However, they also require a secure supporting infrastructure to provide a means of checking they are genuine which does not rely on visual inspection alone. The European Union is leading in this area, with member states required to provide phone-based digital wallets to citizens by the end of 2026. These developments are likely to influence UK approaches to digital identity in the future, requiring the government to consider interoperability, standards and long-term system design choices at an early stage (paragraphs 3.4 to 3.13).

¹ Comptroller and Auditor General, *Challenges in using data across government*, Session 2017–2019, HC 2220, National Audit Office, June 2019; Comptroller and Auditor General, *The challenges in implementing digital change*, Session 2021–22, HC 575, National Audit Office, July 2021; Comptroller and Auditor General, *Digital transformation in government: addressing the barriers to efficiency*, Session 2022–23, HC 1171, National Audit Office, March 2023.

Enablers of delivery

17 Experience from the UK and internationally suggests that implementing digital identity at scale depends on realistic assumptions about timescales and costs, supported by clear decisions on funding, ownership and accountability.

Key decisions, such as which part of government would fund the ongoing operating costs and how responsibilities would be allocated, need to be resolved early.

Delivering digital identity also requires coordination across multiple departments, public bodies and private providers. Combined with long-standing challenges around integrating legacy systems and data, this complexity needs careful navigation to balance ambition with what can be realistically delivered (paragraphs 4.15 to 4.18).

18 The private sector already plays a significant role in digital identity.

International experience highlights the importance of clarity regarding the respective roles of government and private sector providers. In the UK, 275 private sector firms provide services such as right to work, right to rent and disclosure checks. Some government announcements have prompted private sector concerns about its future role. Any future initiative would need to clarify which aspects of digital identity the government may reserve for itself, and which will be delivered by the private sector or duplicate what already exists. This involves being clear about the trade-offs between building public sector capability and supporting an existing market, with implications for cost, delivery risk and private sector participation (paragraphs 2.14 to 2.16, 2.19 to 2.22, 4.10 and 4.24).

Concluding remarks

19 The government has accumulated experience over several decades of work on digital identity. The UK is well positioned to build on what is already in place. This includes the existing legal and technical standards for digital identity and a growing ecosystem of services and providers. The extent to which these can translate into successful outcomes depends on how clearly the government defines any future objectives, delivery choices, and how effectively it addresses long-standing constraints in legacy systems and fragmented data. In any future initiative it will be important to define priority scenarios and set out how to fund, deliver and integrate them across services. It will need to decide how far to build new public sector capabilities, such as a digital wallet and supporting infrastructure, and how far to rely on private sector provision operating within the trust framework. These decisions will shape costs, delivery risk, market participation and the long-term structure of the ecosystem. This will require a clear assessment of value for money across different delivery models.

20 International experience suggests that governments need to give careful thought to the benefits and risks associated with introducing a single personal identifier across multiple services. Doing so would require addressing the practical challenges in integrating with data in legacy systems and the increased security and privacy risks if not designed appropriately. Countries have taken different approaches to managing these trade-offs, drawing on measures such as tokenisation and sector-specific identifiers. Experience also highlights the importance of understanding integration challenges before investing heavily in technology solutions and ensuring that wider business and operational issues are addressed alongside technical delivery.

21 In any future identity initiative, clear criteria for assessing success and realistic delivery timescales will be important in understanding what must be put in place before real benefits to citizen services can be achieved. To deliver value for money, digital identity will need to be both usable and trusted across both public and private sectors, with individuals being able to use it easily, securely and consistently across services. Experience from the UK and internationally shows that this is more likely where the government:

- sets a clear scope and purpose for digital identity, informed by lessons from previous initiatives;
- sets out a clear business case and timetables for any government products or technologies;
- explains its intended role alongside the private sector, including how it will support continued investment and participation; and
- assesses key risks, including low adoption, impacts on existing providers and services, data quality, interoperability and understanding how systems will work together end-to-end to enable prioritisation of what must be done to achieve its aims.