National Audit Office

INSIGHT

Managing digital identity

Department for Digital, Culture, Media & Sport

SESSION 2026-27
2 SEPTEMBER 2026
HC 586

We are the UK's independent public spending watchdog.

We support Parliament in holding government to account and we help improve public services through our high-quality audits.

The National Audit Office (NAO) scrutinises public spending for Parliament and is independent of government and the civil service. We help Parliament hold government to account and we use our insights to help people who manage and govern public bodies improve public services.

The Comptroller and Auditor General (C&AG), Gareth Davies, is an Officer of the House of Commons and leads the NAO. We audit the financial accounts of departments and other public bodies. We also examine and report on the value for money of how public money has been spent.

In 2025, we recognised £2.6 billion of positive financial impacts from our past work through reduced costs, improved service delivery, or other benefits to citizens. This represents about £24 for every pound of net expenditure.

National Audit Office

Managing digital identity

Department for Digital, Culture, Media & Sport

Report by the Comptroller and Auditor General

Ordered by the House of Commons
to be printed on 1 September 2026

This report has been prepared under Section 6 of the National Audit Act 1983 for presentation to the House of Commons in accordance with Section 9 of the Act

Gareth Davies
Comptroller and Auditor General
National Audit Office

26 August 2026

HC 586 | £10.00

Lessons learned reports

Our lessons learned reports bring together what we know on important recurring issues to make it easier for others to understand and apply the lessons from our work.

017952 09/26 NAO

Contents

Summary
Introduction 4

Part One
Understanding digital identity 10

Part Two
What currently exists 21

Part Three
Looking forward 30

Part Four
What is needed to ensure value for money? 34

Appendix One
Our audit approach 39

Appendix Two
Aspects of a coordinated identity system 41

This report can be found on the National Audit Office website at www.nao.org.uk

If you need a version of this report in an alternative format for accessibility reasons, or any of the figures in a different format, contact the NAO at enquiries@nao.org.uk

The National Audit Office study team consisted of:

John Bell, Areti Poleni and Jonathan Pownall, under the direction of Yvonne Gallagher.

For further information about the National Audit Office please contact:

National Audit Office
Press Office
157–197 Buckingham Palace Road
Victoria
London
SW1W 9SP

020 7798 7400
www.nao.org.uk
@NAOorguk

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.

Part One

Understanding digital identity

1.1 Part One describes what digital identity (ID) is, how previous government initiatives have shaped the current landscape, the different ways other countries have implemented digital identity, and the role of digital identity in linking data held in multiple systems and organisations across government.

What is digital identity?

1.2 The government defines digital identity as a digital representation of a person's identity information, such as their name and age. The specific facts about the person are called 'attributes'. Digital means 'held electronically' rather than in a physical form such as a document or ID card. Identity can also include additional details such as an address. It enables people to securely prove things about themselves without needing to present physical documents or disclose unnecessary personal information.

1.3 Digital identity involves a combination of processes, technologies, standards and governance arrangements that together provide confidence about an individual's identity and confirm information about them.

The foundations of digital identity

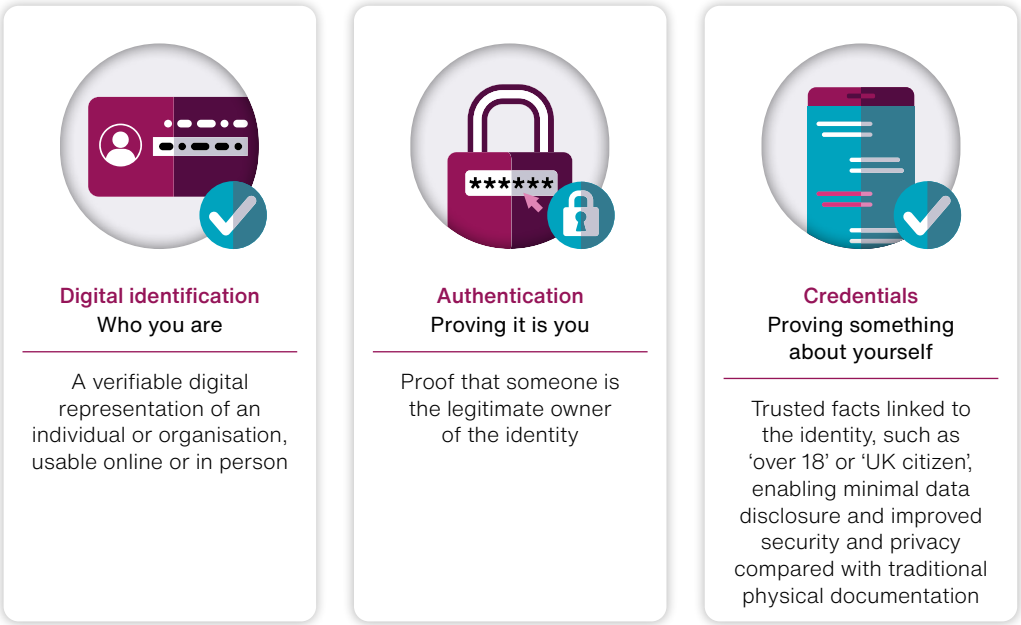
1.4 The foundations of digital identity are who you are, proving the identity belongs to you and proving something about yourself (**Figure 1**).

1.5 Creating a digital identity requires a secure and trusted onboarding process (**Figure 2** on page 12). Such checks typically need a phone capable of reading a passport chip and recording a short video. To avoid exclusion, bias or unfair outcomes, onboarding systems and processes must work consistently across different groups of users and meet accessibility standards.

1.6 The government is already developing and deploying digitally verifiable credentials, which provide secure digital representations of physical equivalents and that respect privacy (**Figure 3** on page 12). For example, the government has announced that it is working on digital driving licences.

Figure 1
The building blocks of digital identity

Digital identification, authentication and credentials serve distinct purposes



Source: National Audit Office review of published information

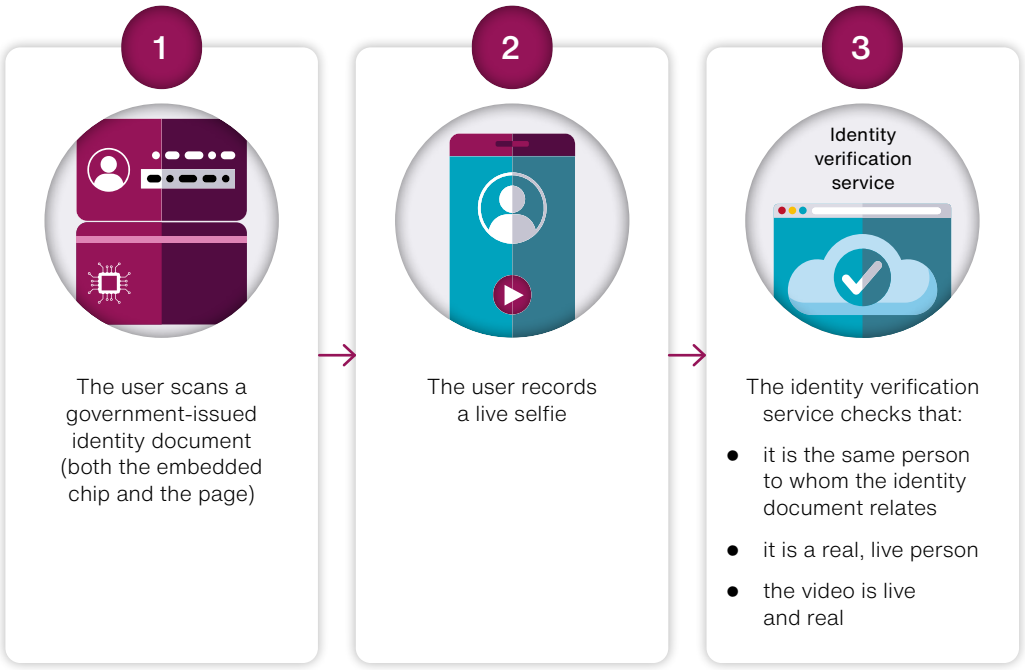
1.7 At present, confirming someone's eligibility for a service typically involves seeking information from an individual and then cross-checking it to decide the outcome. This process can often involve complex data sharing and access agreements between government departments. The introduction of verifiable credentials is likely to have a significant impact on the process as they can provide instant proof of eligibility. However, this is dependent on the availability of a supporting infrastructure to allow a credential to be machine-checked to confirm who issued it and that it has not been forged or tampered with. Proof of authenticity and validity may not be evident from a visual inspection alone (for example, by looking at an image on a phone screen).

Previous UK scope and approaches

1.8 The need for a consistent, reusable way to assure identity and provide a means of secure authentication first came to prominence as the government started to move its services online in the mid-1990s. Without an agreed overall approach, public sector organisations began to develop their own separate solutions. To address this problem, the government started to explore how it could standardise ways to verify the identity of individuals and organisations and provide a secure and trusted means for individuals to sign-in.

Figure 2
Digital ID secure onboarding overview

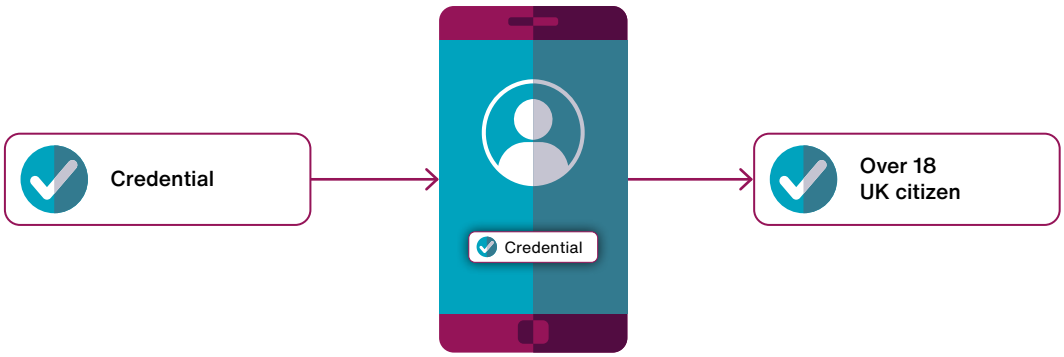
The onboarding process for a digital ID involves three main steps



Source: National Audit Office review of published information

Figure 3
Verifiable credentials separate data sharing from source systems

Information can be verified without accessing original databases



Issuer

Creates and signs the credential (e.g., a university, employer, government department)

Holder

Stores the credential in a digital wallet and controls when/how it is shared

Verifier

Checks authenticity and validity using trusted digital infrastructure

Source: National Audit Office review of published information

Cross-government digital identity approaches

1.9 The government has adopted several approaches to digital identity over time. Initiatives have ranged from the use of public and private sector providers, as with Government Gateway from 2001, to state-issued national identity cards (2006–2010), exclusive reliance on commercial identity providers (2014–2023), and more recent proposals for a return to a mixed environment (**Figure 4**).

Figure 4
UK Government's approach to digital identity, 2001 to 2026

Similar objectives have been pursued through different delivery models

Initiative	Dates	Intended purpose	Notable facts
Government Gateway	2001–present	A cross-government identification, authentication and single sign-in platform for citizens, businesses and delegates (people acting on behalf of others). At launch, approved commercial organisations provided digital identity and authentication services alongside the government's own service. Later, only the government service remained available.	At its peak in 2011, it was supporting 227 public sector services. These started to be withdrawn, and its use restricted to HM Revenue & Customs (HMRC) services, during the development of GOV.UK Verify. In March 2019, HMRC decommissioned the original Government Gateway infrastructure and services were migrated to replacement systems. However, people still use a Government Gateway user ID to log in to HMRC's replacement system. From April 2024 to March 2025, over 56 million accounts were used 435 million times to access services.
National Identity Scheme	2006–2010	The National Identity Card and National Identity Register included helping "employers find out about the immigration status of job applicants and about any visa restrictions which mean they cannot legally work in the UK."	Fewer than 15,000 national identity cards were issued during the lifetime of the programme. The ID scheme was cancelled in its entirety by the coalition government in 2011, who said their aim was "to reverse the erosion of civil liberties."
Identity Assurance Programme and GOV.UK Verify	2010–2023	A cross-government identification, authentication and single sign-in platform for citizens. It relied exclusively on approved commercial organisations to verify and manage people's identities.	In July 2018, the Infrastructure and Projects Authority concluded that successful delivery of the project was unachievable and recommended that Verify be closed as quickly as practicable. At the time of its closure, GOV.UK Verify had "almost 10 million user accounts and ... 27 different online government services."
GOV.UK One Login	2021-present	A cross-government identification, authentication and single sign-in platform for citizens.	A GDS blog stated in January 2026 that "over 13 million people have already used it to access more than 120 different services."

Source: National Audit Office analysis of published information

Proposals for UK digital ID

1.10 In September 2025, the UK Government announced initial proposals for a digital identity system, including a digital ID and supporting infrastructure such as a digital wallet. In March 2026, the government consulted on a voluntary, free-to-use digital ID that would have been stored in the GOV.UK Wallet on a person's phone and built on existing systems such as GOV.UK One Login. In July 2026, the government announced that it would not proceed with proposals for a government-issued digital identity card.

1.11 In May 2026, the government announced the introduction of a Digital Access to Services Bill, with the headline objective to modernise how citizens interact with public services. While policy regarding digital identity has subsequently evolved, questions around the role of digital identity in public service delivery remain highly relevant.

International approaches

1.12 Internationally, three broad models can be observed:

- **State-led models,** where governments issue and govern digital identity. Estonia and Singapore are commonly cited examples of this approach. In Estonia, a mandatory state-backed digital identity is used across public and private services, supported by strong legal controls, auditability and transparency over data access. Singpass is Singapore's national digital identity system that enables residents to securely access a wide range of government and private sector services.
- **Co-regulated or partnership models,** where the state sets standards and oversees the private providers who deliver services. Denmark and Norway have taken this approach. In Denmark, digital identity is jointly governed by government and the banking sector and widely used across both. In Norway, bank-issued BankID has become the de facto national digital identity, supported by statutory backing and financial sector assurance standards.
- **Plural provision within a shared set of trust rules,** where governments define requirements but allow multiple public and private providers to issue or rely on digital identities. Australia and the European Union (EU) follow this approach. In Australia, a government-run core system operates alongside accredited private providers. In the EU, the EU Digital Identity framework (**Figure 5**) allows public authorities and recognised private institutions to issue credentials within a shared legal and technical framework.

Figure 5

The European Digital Identity (EUDI) framework and digital wallet, as at April 2026

The EUDI framework sets the rules for digital identity across the European Union (EU), while the wallet allows individuals to store and use their identity information

How the EUDI framework works:

- The EU sets the legal and technical rules for digital identity.
- Member states and authorised providers issue digital identity credentials within this framework.
- Individuals store and use these credentials through a digital wallet on their phone.

What the wallet does:

- Provides a secure way for individuals to store and manage their digital identity.
- Contains personal identification data (PID), such as name and date of birth, issued by a member state or authorised provider.
- Allows individuals to share only the information needed for a transaction (for example, confirming age without sharing date of birth).
- Enables individuals to log in securely to services, create electronic signatures and record transactions.

Note

1 EU member states are required to make at least one European Digital Identity (EUDI) wallet available by the end of 2026.

Source: National Audit Office analysis of published information

1.13 Across these models, trust frameworks are critical. They define who can issue identities or credentials, the standards they must meet, who is responsible if something goes wrong and how data is protected. Arrangements are becoming more structured with laws, certifications and regulators ensuring things are done properly. This enables digital identities to be reused safely across organisational boundaries and between sectors.

1.14 International evidence indicates a shift in some countries away from highly centralised, state-operated identity systems towards ecosystems in which governments set rules and create the conditions for trust, while private providers play a significant role in delivery and adoption (**Figure 6** overleaf). The effectiveness of these systems is linked to clarity, credibility and enforcement of the underlying trust framework, with take-up relying on systems that people trust, and that protect privacy and work reliably across both public and private sectors.

Figure 6

International approaches to digital identity for selected countries, as at April 2026

Approaches vary in state control and private provision

Country	Public and private sector roles
Australia	Operates a hybrid model. Government provides the core digital ID system and governance, while accredited private sector providers are being brought into the ecosystem to expand choice and coverage.
Denmark	Co-regulated partnership between the state and the banking sector. It is widely used across both public services and private markets, particularly financial services.
Estonia	State-led model, with government issuing and governing digital identity, but allowing extensive use across both public and private services.
France	Approach is state-centric, with government providing and governing digital identity while enabling reuse across public services and some private sector transactions.
India	Highly centralised, state-issued identity system, which is widely relied upon by both government and private sector organisations, particularly in financial services.
Norway	Private sector led, co-regulated model. Banks collectively issue and operate the national digital ID, which is relied upon by government and industry alike.
Poland	Combines a mandatory state identity with widespread use of bank-issued digital IDs. In practice, the private sector plays a major operational role in digital identity usage.
Singapore	Strongly state-led model, with a mandatory digital identity provided by government and used across both public services and private businesses.

Source: National Audit Office analysis of Supreme Audit Institutions data

1.15 International experience suggests that where digital identity has delivered broader benefits, these have often arisen from its integration with existing systems, data and infrastructure, rather than from the identity credential alone. For example, the Estonian government's ID is often cited as modern, secure and citizen-centric. Yet its value derives not only from the ID itself but from other closely integrated aspects, including:

- joined-up data access across government, which reduces duplicate paperwork and allows instant access to reliable information;
- support for electronic signatures, allowing citizens to sign documents online; and
- a commitment to transparency and trust, letting citizens see when officials have accessed their data.

Identity as a means of joining up public services

1.16 The UK's policy objectives for digital identity have remained broadly consistent over time, although their relative emphasis has varied:

- tackling illegal working and immigration abuse;
- disrupting use of false and multiple identities by organised criminals and terrorists;
- protecting people from fraud and ID theft;
- ensuring free public services are only used by people entitled to them; and
- allowing easier and more convenient access to public services.

1.17 The government's broader proposals for digital transformation have placed an emphasis on joining up public services. There are three distinct and separate challenges involved in using digital identity to support joined-up services (**Figure 7** overleaf):

- **verification** – confirming that an identity exists and belongs to the person claiming it;
- **matching** – linking that verified identity to the correct customer record within a specific system; and
- **linking** – connecting the same individual across multiple systems that may represent them differently.

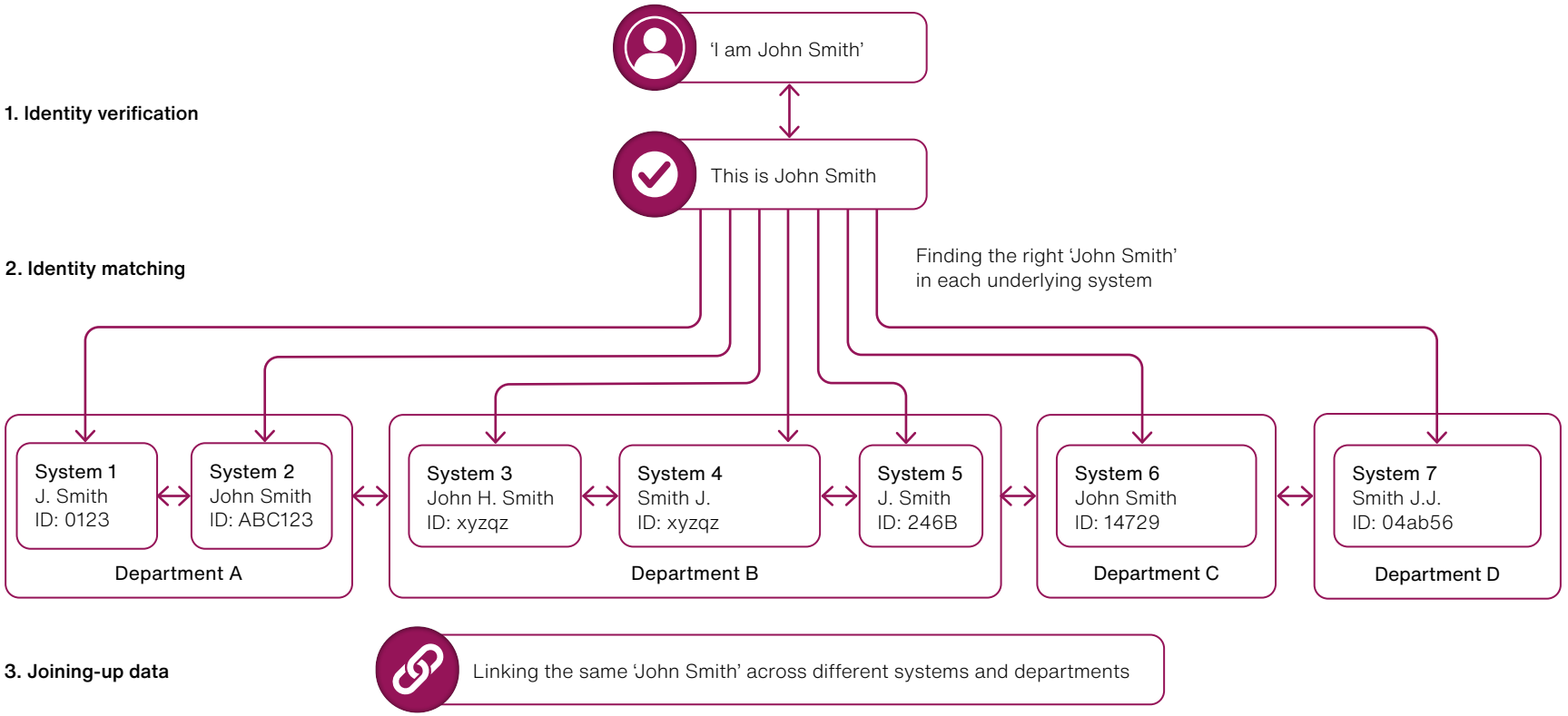
Data linking and matching

1.18 Progress depends not only on establishing a trusted digital identity but also on how that identity can be linked to, and reconciled across, the existing systems landscape. This is not straightforward where data and records are held across multiple organisations, services and systems, often in different formats and of varying quality (**Figure 8** on page 19).

1.19 Our previous reports have identified persistent barriers, including structural silos between departments, unclear ownership and difficulties integrating data and systems. Legacy platforms, inconsistent standards and multiple representations of the same individual across systems have all constrained the ability to connect data effectively across services. For example, in our report *Progress with Making Tax Digital*, we said that while HM Revenue & Customs's corporation tax system was operationally stable it could not easily be adapted to support the single taxpayer record and that corporation tax had been descoped from the Making Tax Digital programme until at least 2030. Such an environment would be a practical constraint on how far a future digital identity initiative could help join up public services.

Figure 7
Verification, matching and linking

Verifying someone's identity, matching it to a record in a system and linking records relating to the same identity across different systems are separate problems to be solved



Note

1 In the above figure, names and reference numbers relating to the same individual are deliberately shown as being inconsistent and, in some cases, incorrect.

Source: National Audit Office analysis of published information

Figure 8
UK Government sector-specific identifiers

As at April 2026, UK public services use different forms of identifiers

Area	Identifier	When issued	Purpose
Healthcare	NHS Number	At birth or on first contact with a GP	Patient records
Travel	Passport Number	On application (but the number changes on every passport renewal or reissue)	Internationally recognised travel document
Pensions and benefits	National Insurance Number (NINO)	Created when a Child Benefit claim is made, but not notified until three months before someone's 16th birthday; on application	Tax, benefits, employment
Tax	Unique Taxpayer Reference (UTR)	On registering for Self-Assessment or setting up a limited company	Tax self-assessment
Education	Unique Learner Number	Issued by schools or colleges to learners aged 14 or over	Learner tracking
Driving	Driving Licence Number	On first application for a provisional driving licence	Driver records
Birth certificate	Certificate number, General Register Office reference number	Issued when a birth is registered; births in England, Wales and Northern Ireland must normally be registered within 42 days of birth	Proof of birth and parentage

Note

1 There are three separate NHS Number systems: one for England, Wales and the Isle of Man; one for Scotland; and one for Northern Ireland.

Source: National Audit Office analysis of published information

Single personal identifiers across government

1.20 Approaches to addressing matching and joining up also raise issues and risks where systems rely on common identifiers. Identity systems handle some of an individual's most sensitive personal information. Poor design or implementation can heighten the risks of data breaches, fraud and other misuse, particularly where the same identifier is stored and reused across multiple systems and organisations.

1.21 One method increasingly used to mitigate such risks is tokenisation, which allows sensitive information to be handled securely without sharing the underlying central identifier. This reduces the risk of it becoming more widely known or compromised in a data breach, thus also helping to reduce the risk of identity theft.

1.22 Several governments already use tokenisation in digital identity systems. In India, following earlier data breaches, users can now generate temporary tokens to replace the Aadhaar number for authentication and 'know your customer' checks. Austria issues sector-specific tokens that enable authorised use without allowing data to be linked across services. By contrast, in the United States, the widespread reliance on the Social Security Number as a single master identifier has made it vulnerable, as it is stored across multiple, potentially insecure databases and is therefore a frequent target for data breaches and fraud.

Part Two

What currently exists

2.1 In Part Two we describe the current digital identity landscape in the UK, including the roles of government and the private sector.

Organisations and roles

2.2 Government involvement in digital identity spans legislation, policy, standards and direct delivery. This includes the development of products (such as GOV.UK One Login), the development of the digital verification services market and policy relating to the adoption of digital identity across the economy.

2.3 A wide range of organisations are involved with digital identity in the UK (**Figure 9** on pages 21 and 22 and **Figure 10** on page 23).

Figure 9
Organisations involved with digital identity in the UK, as at July 2026

Digital identity responsibilities are distributed across government

Organisation	Role
Department for Digital, Culture, Media & Sport (DCMS)	Policy responsibility for digital identity.
Government Digital Service (part of DCMS)	GOV.UK One Login (single sign-in for online services for individuals) and GOV.UK Wallet (secure credential store).
Office for Digital Identities and Attributes (OfDIA) (part of DCMS)	Enable the use of digital identity and attributes across the economy; operate the provisions of the Data (Use and Access) Act 2025, including maintaining the trust framework, assurance processes, trusted services register and legal framework for data sharing; and oversee the trust services regime with operational responsibilities delegated to the Information Commissioner's Office.
HM Revenue & Customs (HMRC)	Government Gateway (single sign-in for HMRC online services for individuals, businesses, and those with delegated authority) – currently only the single sign-in for new tax individuals is transitioning to GOV.UK One Login as part of HMRC's 2025/26 to 2029/30 Transformation Roadmap.
Home Office (including HM Passport Office)	Passports, eVisas, right to work and right to rent digital share-codes.
Driver & Vehicle Licensing Agency (DVLA)	Driving licences (digital versions in development). DVLA covers Great Britain licences only – Northern Ireland manages its own.

Figure 9 *continued*
Organisations involved with digital identity in the UK, as at July 2026

Organisation	Role
Office for Veterans' Affairs (part of the Ministry of Defence)	Veterans Card and digital card.
Ministry of Housing, Communities & Local Government (MHCLG)	Working with local authorities on the potential use of GOV.UK One Login.
NHS	NHS login (single sign-in for patient access to digital NHS services).
National Cyber Security Centre	Standards for secure authentication methods and identity systems.
Information Commissioner's Office	Operational responsibility for eIDAS (e-signatures, etc.) and General Data Protection Regulation.
Financial Conduct Authority	Regulation of banks (including 'know your customer' checks) and Open Banking (which uses digital identity and authentication services).
Local authorities	Responsible for their own requirements. Work is taking place with MHCLG and GDS Local on the potential use of One Login.
ScotAccount	Identification, authentication, and single sign-in for Scottish Government services.
nidirect	Northern Ireland single sign-in services.
Digital sector: Digital Verification Service (DVS) providers	Digital identity providers (e.g. identity proofing, age verification, right to work/rent checks).
UKAS – The UK Accreditation Body	Accredits the certification bodies that ensure providers' compliance with the DVS framework.
BSI and Kantara	The organisations currently approved to evaluate and certify providers against the DVS framework (other organisations may join the certification scheme).
Home Office, Chartered Trading Standards Institute, National Police Chiefs' Council	Proof of Age Standards Scheme (PASS), the national accreditation scheme for proof of age cards.

Notes

1 Following machinery of government changes announced in July 2026, responsibility for digital identity policy moved from the Cabinet Office to the Department for Digital, Culture, Media & Sport (DCMS). The Government Digital Service (GDS) and the Office for Digital Identities and Attributes (OfDIA), previously part of the then Department for Science, Innovation and Technology (DSIT), also transferred to DCMS.

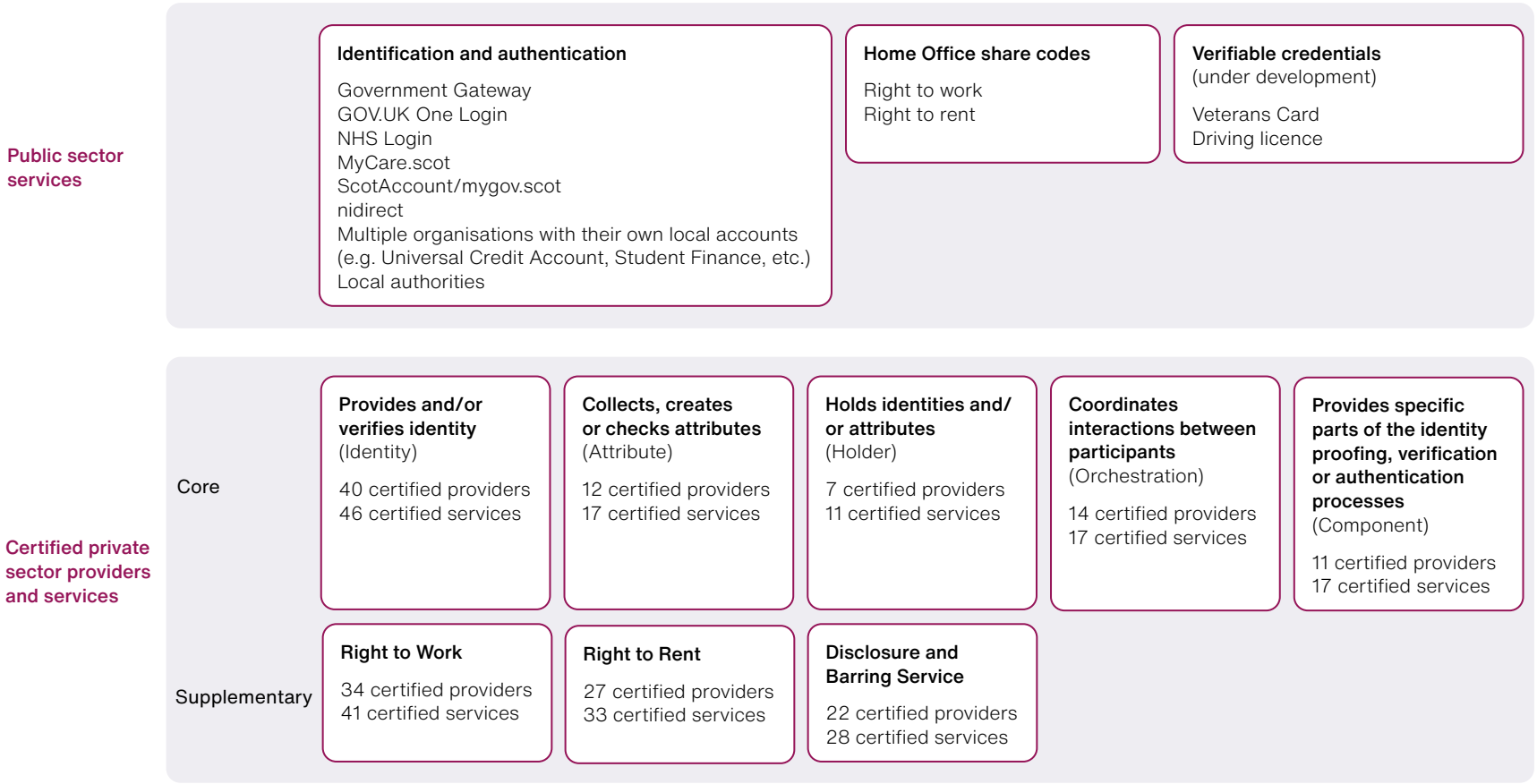
2 Digital Verification Service (DVS) is a service that enables people to prove who they are, information about themselves or their eligibility to do something. A list of digital verification services is available at www.digital-identity-services-register.service.gov.uk

Source: National Audit Office analysis of government data

Figure 10

UK's digital identity and authentication landscape

Digital identity spans public sector systems and private markets (as of 3 August 2026)



Notes

1 The digital verification services trust framework defines five roles for digital identity organisations and services: identity service provider, attribute service provider, holder service provider, orchestration service provider and component service provider. The numbers in the figure show the count of certified providers and services in each category.

2 MyCare.scot is a digital service that brings together health and social care information. To use MyCare.scot, users need a verified ScotAccount. ScotAccount is a service run by the Scottish Government that allows users to verify their identity for public services. mygov.scot is a platform for accessing public services in Scotland.

3 nidirect is the official government website for Northern Ireland residents bringing together information from government departments and agencies.

Source: National Audit Office analysis of published information

Public sector services

2.4 This section describes existing public sector identity-related services and initiatives. Overall, the UK public sector has a wide range of identity-related services, such as passports, driving licences, Government Gateway, GOV.UK One Login, NHS Login and others. However, these have been built in silos, operate at different assurance levels and are not fully interoperable. Key aspects (such as integration across services, use by local authorities and handling of multiple accounts) are still evolving.

Passports and driving licences

2.5 As state-issued documents confirming citizenship or nationality, passports are frequently used when someone needs to prove who they are. Passports are widely held. The 2021 census shows that 45.7 million UK residents held a UK passport, equivalent to around 77% of the population. UK passports include a machine-readable chip which stores the information shown on the passport's photo page, including a digital facial image. Some government services, such as GOV.UK One Login, can use smartphones to read passport chips.

2.6 Although driving licences are not officially classed as identity documents, they are widely used to prove name, age or address, as well as the entitlement to drive. More than 42 million are in circulation in Great Britain. Proposals for a digital driving licence first appeared in 2016, when the Driver & Vehicle Licensing Agency (DVLA) demonstrated a prototype, although this was solely an image of the licence rather than a digital credential. In January 2025, the government announced that people would soon be able to acquire a digital driving licence stored on a phone.

Government Gateway, GOV.UK One Login and GOV.UK Wallet

2.7 Government Gateway provides identification, authentication, and single sign-in for citizens, businesses and delegated access by intermediaries to HM Revenue & Customs (HMRC) services. Between April 2024 and March 2025, it had over 56 million active accounts and was used 434.9 million times. Although now mainly used for tax-related services, it also allows people to view information such as their National Insurance record and State Pension forecast. For individuals, Government Gateway is being replaced by GOV.UK One Login, although plans for businesses and delegated access (such as for accountants) remain unclear.

2.8 GOV.UK One Login lets a user prove their identity once and then access multiple government services through a verified account. It operates at a mid-level of identity assurance.[2] This represents an increased level of confidence for most services in comparison to what was in place previously. Some services require higher levels of confidence, such as Disclosure and Barring Service (DBS) checks. While users are not blocked from creating multiple GOV.UK One Login accounts (for example, to separate business and personal activity) the vast majority of users have one account.

2.9 The GOV.UK Wallet is being developed for people to securely store digital versions of government-issued documents on their phone. Use will be optional and secured through GOV.UK One Login. Government policy is that, over time, digital versions of credentials will be issued alongside paper or plastic versions. How multiple GOV.UK accounts will work alongside the GOV.UK Wallet is still evolving.

Other public sector identity services

2.10 Local authorities generally operate their own systems and processes for identity checks and online authentication. Central government has recognised that this creates duplication and challenges for both users and councils. Work is underway to explore whether GOV.UK One Login could play a wider role.

2.11 NHS Login provides identification, authentication and single sign-in for NHS patient services. As of June 2026, more than 45 million people were registered. Different levels of identity checking are used depending on the service accessed. There is no link or interoperability between NHS Login and GOV.UK One Login.

2.12 ScotAccount provides identification, authentication and single sign-in for Scottish Government services. Since launching in February 2023, over 540,000 accounts have been created, with more than 2.2 million sign-ins. Residents of Northern Ireland access devolved public services online through the nidirect website.

Right to work and right to rent checks

2.13 Checks on someone's right to work or rent rely on a UK or Irish passport or, for people without British or Irish citizenship, a digital share code issued by the Home Office. A share code is a temporary code that a person who holds a digital immigration status generates online and gives to an employer or landlord. When entered into the official Home Office online checking service, the code shows whether the person has permission to work or rent, along with any conditions or expiry dates. It has replaced earlier physical documents, such as visas and biometric residence permits.

2 Digital identity services register, available at www.digital-identity-services-register.service.gov.uk.

Trust frameworks and standards

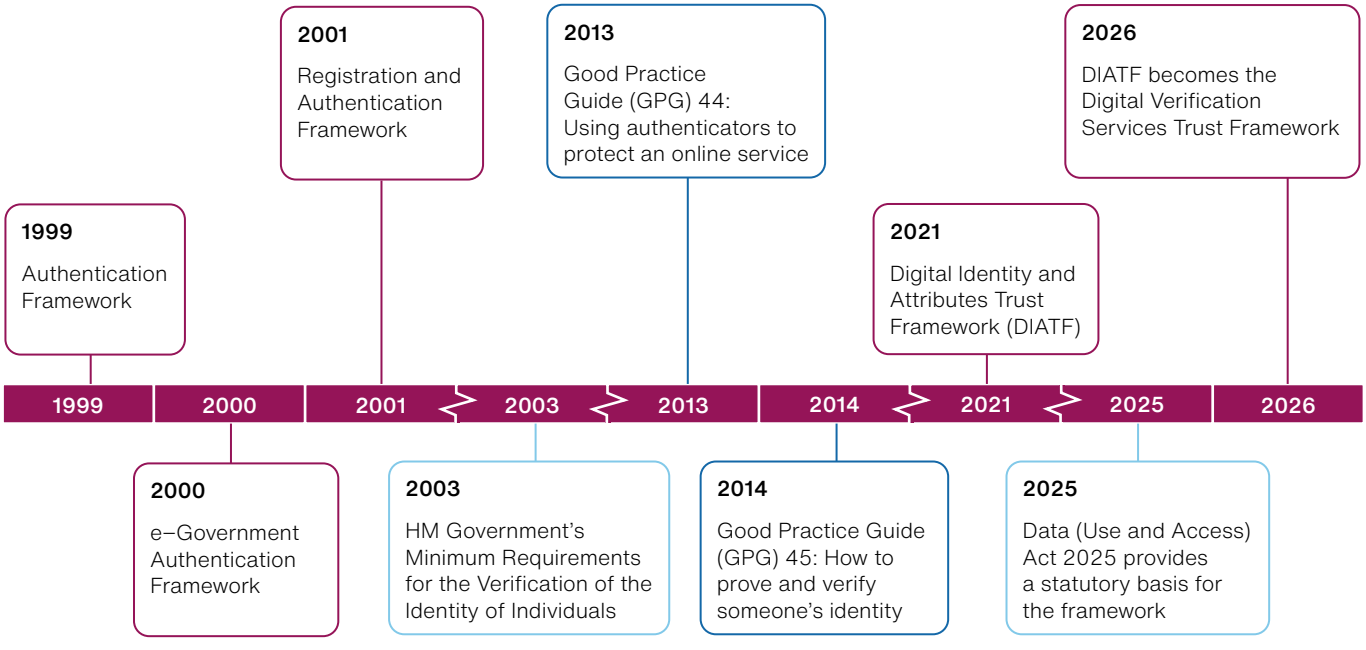
2.14 The government has published guidance and frameworks relating to authentication and identity assurance since 1999 (**Figure 11**). The Digital Verification Services (DVS) trust framework is the first digital identity trust framework to be placed on a statutory basis under the Data (Use and Access) Act 2025. It establishes trust and consistency both in the level of identification of an individual and the strength of the credential used to authenticate them. Compliance is assessed through a formal scheme supported by accredited assessment bodies.

2.15 Four levels of assurance for identity services have broadly persisted since the original framework, reflecting the fact that not all services need the same degree of assurance. Today's assurance levels range from 'low confidence', suitable for low-risk transactions, to 'very high confidence', to protect against advanced fraud.

Figure 11

UK Government frameworks, guidance and requirements relating to authentication and digital identity, 1999 to 2026

The government has published guidance and frameworks on authentication and identity assurance since 1999



Source: National Audit Office analysis of published information

2.16 The framework also sets out different roles and responsibilities for identity providers. They include confirming who someone is (identity service providers) and managing specific pieces of information about a person, such as their age or qualifications (attribute service providers).

Digital trust services and eIDAS

2.17 In the EU, the Electronic Identification, Authentication and Trust Services (eIDAS) regulation provides a regulatory framework to standardise digital identity and trust services. The UK's retained version of eIDAS sets the legal framework for trusted services such as electronic signatures, time stamps, electronic documents and website authentication. The Information Commissioner's Office oversees trust services, including recognition of overseas electronic signatures and compliance enforcement.

2.18 The framework enables important functions such as signing contracts electronically. This could offer significant benefits for everything from contracts to purchase orders and invoices. Decisions about whether to integrate functions such as legally recognised electronic signatures will shape how useful a digital identity will be for the UK.

Private sector initiatives

2.19 As of 2025-26, 275 firms were involved in digital identity services. Some focus on checking who someone is or confirming specific details about them, such as their age. Others provide tools to create and manage digital identities, verify documents or use biometric checks such as facial recognition. Some of these firms also provide services that presently sit outside of the trust framework (for example, age estimation services).

Providers certified under the trust framework

2.20 Those digital identity providers who choose to be certified against the DVS trust framework for in-scope services are listed in an official register published under powers in the Data (Use and Access) Act 2025. As at 29 June 2026, it listed 64 certified services from 47 providers.

2.21 Certification indicates that a provider or service meets the framework's standards. Certified services include checks related to the right to work or rent, age verification, and sharing of specific attributes. Individuals using certified services typically verify their identity once and then reuse it when needed, subject to the right policy, regulatory and technical conditions being in place. If they are not, this may undermine the potential benefits of such reuse.

Open banking

2.22 Digital identity and authentication also play an important role in banking, supporting regulatory requirements such as age verification and 'know your customer' checks. Open banking allows people and businesses to grant secure, time-limited access to their bank account information (for example, to confirm account existence and ownership or to view multiple accounts in one place).

Challenges to the wider use of digital ID

Acceptance

2.23 Despite the existence of a wide range of digital identity providers and services, UK law does not require organisations to accept digital identity. Most retailers, for example, still rely on physical documents. Organisations may lack familiarity with digital identity or the tools to verify its validity and authenticity. In other areas, such as voter identification at polling stations, digital ID is not accepted, even from certified providers, with the exception of the digital Veteran Card[3] and e-visas. To improve the usability of digital identity, in June 2026, the Home Office laid regulations to allow customers at licensed premises in England and Wales to prove their age using digital checks from registered digital verification service providers. These changes will enable customers to use digital identity to prove they are old enough to buy alcohol, as an alternative to presenting a passport or driving licence.

Support for delegated authority

2.24 Delegated authority is an integral aspect of how identity works in the real world. Many individuals and businesses rely on others to act on their behalf, such as carers, family members, professional agents and employees. These arrangements have traditionally been supported through paper mandates or informal processes. While digital identity is often designed around individual users, delegated authority remains only partially supported across government services. One reason some organisations could not adopt GOV.UK Verify was that support for businesses and people acting on behalf of others was removed from the scope of the programme, limiting its use in contexts such as accountants managing tax for clients. Systems that do not adequately support lawful delegation can risk excluding people or requiring instead parallel, non-digital workarounds.

3 The digital Veteran Card is a government-issued digital version of the HM Armed Forces Veteran Card, being introduced via GOV.UK One Login and used to prove an individual's veteran status.

Digital inclusion

2.25 Digital services have to consider how to address the issue of citizens without a digital footprint. The Department for Work & Pensions (DWP) has looked at solutions over a number of years for people who are digitally excluded and has developed ways of addressing this. It uses multiple identity verification routes to cover most individuals, including knowledge-based verification drawing on DWP and HMRC data. Alongside online channels, DWP offers face-to-face assistance for those who require it or do not have the necessary documentation to prove their identity online. GOV.UK One Login offers DWP customers an assisted digital route through the Post Office, and Job Centres can verify a customer's identity using a variety of methods, including vouching where necessary. The Data (Use and Access) Act 2025 allows DWP to share information with trusted partners and DVS-registered providers, enabling them to widen verification options. These data sharing powers are exclusively permission-based: a person must request that their data is used to perform identity or eligibility checks. Inclusion considerations also extend beyond initial access to digital identity, and cover ongoing usability, the ability to obtain help and the confidence to manage digital credentials over time.

Part Three

Looking forward

3.1 In this part we describe how the digital identity landscape is likely to develop in future, focusing on emerging international standards, mobile-based technologies such as digital wallets and verifiable credentials, and how these developments could shape the UK's options and design choices.

International developments

3.2 Standards developed by the International Civil Aviation Organisation (ICAO), the International Organisation for Standardisation (ISO), and the World Wide Web Consortium (W3C) play an increasingly important role in digital identity systems. They include requirements for digital passports, digital driving licences and verifiable credentials, which improve how individuals can obtain, store and share verified personal information in a way that minimises disclosing unnecessary data.

3.3 This combination of standards and familiar technology, if correctly applied, gives governments a route to digital identity that is interoperable, privacy-preserving and more resilient to misuse.

Digital passports

3.4 ICAO's standards for Digital Travel Credentials (DTCs) define three types (**Figure 12**).

3.5 The standards for DTCs for mobile (e.g. phone-based) use for Types 2 and 3 above are still being developed. In the United States, iPhone users can set up a Type 1 DTC, the most limited form, for use at selected airport security checkpoints for domestic travel, including for age and identity checks.

Figure 12

Types of International Civil Aviation Organisation (ICAO) Digital Travel Credentials (DTCs), as at April 2026

DTCs range from digital versions that still rely on a physical passport to fully digital documents

Type	Description
1	Created from a physical passport's chip data, but still requires the passport to be carried
2	Issued by the passport authority as a digital credential linked to a passport, and typically used alongside the physical passport
3	A fully digital passport that can be used without needing a physical document

Notes

1 The International Civil Aviation Organisation (ICAO) has developed standards for Digital Travel Credentials to allow people to prove their identity when travelling in a digital format, using securely shared digital passport information.

2 Standards are already defined for all DTC types and can be issued today using smartcards. Mobile (phone-based) versions are not yet finalised.

Source: National Audit Office analysis of International Civil Aviation Organisation information

Digital driving licences

3.6 Digital driving licences are further advanced than passports. The international standard defines how a driving licence can be issued as a secure digital credential stored on a phone. An organisation relying on the licence can check that it is genuine and unaltered.

3.7 The UK government announced plans to introduce digital driving licences from 2025. In the United States, digital driving licences are already issued by some states and accepted as a form of identity at more than 250 US airports. Some states use commercial wallets, such as those provided by Apple or Google, while others require their own dedicated app or wallet.

Verifiable credentials

3.8 As described in Part One, a verifiable credential is a digital statement, such as 'this person is over 18', that can be checked to confirm who issued it and that it has not been tampered with. Verifiable credentials are internationally standardised by the W3C. In the UK, the Government Digital Service is responsible for defining a common public sector approach and developing a central infrastructure to support the issuance of verifiable credentials and their use across the public sector. The Office for Digital Identities and Attributes is guiding the use and creation of these credentials in both the public and private sectors by virtue of its role maintaining the UK digital verification service (DVS) trust framework.

Mobile-based technology

3.9 Mobile technology is central to future digital identity because it offers a secure and familiar way for people to manage their identity. Smartphones act as personal identity tools, using built-in features such as biometrics and secure hardware to support strong authentication. This supports how digital wallets work.

Digital wallets

3.10 A digital wallet acts as a secure place to store multiple digital items on a phone, including identity credentials issued by different organisations. Instead of repeatedly entering details or creating separate accounts, individuals can use a wallet to hold verified digital documents and share only the information needed for a particular purpose. The wallet manages security and consent through encryption and secure storage, with the user approving which apps and services access which information.

3.11 Digital wallets support various uses, including:

- **payments**: bank cards for contactless payments;
- **memberships and tickets**: for example, loyalty cards, travel and event tickets; and
- **digital identity**: including digital driving licences.

3.12 A verifiable credential stored in a digital wallet is still reliant on a supporting infrastructure to enable it to be verified. For example, travel and event tickets are routinely machine read by a dedicated scanner or a phone-based app to check that they are genuine and have not been duplicated or used already.

3.13 Phone-based digital identity is becoming more prevalent in a number of countries, either replacing or complementing traditional smartcard-based ID (**Figure 13**). In the European Union, member states are required to implement the European Digital Identity (EUDI) wallet, underlining how identity systems are evolving to include phone-based digital identity. The EUDI approach includes a secure digital wallet that can acquire, store and use verifiable credentials with selective disclosure.

Figure 13

Phone-based approaches for selected countries, as at April 2026

Digital wallets are becoming more prevalent

Country	Role of digital wallets
Australia	Australia is moving towards wallet-based identity. The policy direction supports multiple wallets and providers, operating within common accreditation and interoperability rules.
Denmark	Denmark is transitioning to a national digital ID wallet, intended to store credentials and support selective disclosure. The wallet remains voluntary and reinforces user control.
Estonia	Estonia is evolving towards wallet-style functionality layered on top of its existing state identity infrastructure. Wallets are positioned as an extension of the state identity system, rather than a separate market-driven product.
France	France supports a government-provided digital wallet, designed to complement rather than replace physical ID. The wallet is optional and framed as a convenience tool operating as part of France's official state digital identity system.
India	India has enabled wallet-like uses of identity credentials, but within a state-controlled identity ecosystem rather than an open, multi-provider wallet model.
Norway	In Norway, digital identity is closely tied to bank-provided apps, which function in practice as wallets for authentication and signing. There is no separate state wallet and trust is inherited from the banking ecosystem.
Poland	Poland has introduced a state-provided digital wallet, with the same legal standing as the physical ID card. This approach positions the wallet as a core instrument of state digitalisation and not an optional add-on.
Singapore	Singapore provides a single, government-operated digital wallet, tightly integrated with national services and private sector use cases, reinforcing a unified national identity layer.

Note

1 As EU member states, Denmark, Estonia, France and Poland are required to provide at least one European Digital Identity Wallet by the end of 2026.

Source: National Audit Office analysis of Supreme Audit Institutions' data

Part Four

What is needed to ensure value for money?

4.1 This part discusses the foundations and challenges associated with digital identity and the factors conducive to achieving value for money.

Foundations

4.2 The UK government already has several decades' experience of work on digital identity. This includes insights from the operation and user experience of public sector identification and authentication services, the growing use of certified private sector verification service providers and the experience of developing trust frameworks to set consistent standards of identity assurance and accreditation.

4.3 International experience provides useful insights, including how to encourage take-up by citizens and business by integrating digital ID with better public and private sector processes and services. Well-designed digital identity can enhance security and privacy and reduce fraud through data minimisation and mutual verification between parties to a transaction.

Challenges and risks

4.4 Despite these foundations, any future initiative involving digital identity would face significant challenges in achieving value for money. As we have previously reported, the government has a mixed track record in delivering large scale transformation. Adequate funding and realistic timetabling are key, together with clarity on funding, ownership and implementation responsibilities.

4.5 In our report *The challenges in implementing digital change*, we said that digital change involves high levels of complexity, uncertainty and risk, which are often unique to each specific programme due to legacy data and systems, existing operations and the difficulties of integration. In the 2025 state of digital government review, the government accepts that it continues to face persistent systemic challenges in modernising public services. These include institutionalised fragmentation; long-standing legacy, cyber and resilience risks; inconsistent leadership; a skills shortfall; and outdated funding and purchasing models.

4.6 There are also unresolved policy and implementation questions which will take time to think through. These include how verifiable credentials will be revoked in a way that is legally robust and avoids unintended and unforeseen consequences (for example, where revocation could prevent an individual from accessing essential services, meeting legal obligations or proving entitlement, through no fault of their own). Other questions include how authoritative systems of record will be maintained; how legal liability and accountability will be managed across multiple parties; and how the government will monitor costs and benefits given its limited track record in this area.

4.7 Finally, efforts to enable digital identity require coordination across central government, devolved administrations, local government and the private sector, potentially in different states. This need to span sectors and nations increases the complexity of any future approach to digital identity and raises further challenges around accountability, responsibility and interoperability.

Characteristics of successful approaches

4.8 International experience suggests some common characteristics shared by digital identity systems with higher levels of adoption. We set these out more fully in the following section. They include a clear statutory and policy framework; clarity of purpose and scope; sustainable funding and resourcing; compelling and high-value use cases; and strong security, privacy and accountability protections that avoid single points of failure.

4.9 UK and international experience indicates that digital identity is unlikely to deliver significant economic and social benefits without wider reforms. Countries regarded as successful have combined digital identity with broader transformation, including interoperable data infrastructure, electronic signatures, simplified administrative processes, improved citizen privacy and official accountability.

4.10 Systems with higher adoption tend to define clearly the role of public and private sectors; ensure strong compliance and adoption across the public sector; engage stakeholders effectively to build trust; work reliably; and embed transparency and accountability mechanisms that allow citizens to understand how their data is used.

Insights for achieving value for money

4.11 Achieving value for money requires effective coordination across a range of factors, from stakeholder engagement to legislation to technical design and implementation. Below and in Appendix Two we summarise the UK Government's status relative to the characteristics of successful approaches that we outline above. We intend the observations below to be a useful contribution to understanding the current position.

Legal and policy framework

4.12 International models show liability, accountability and data access rules are typically embedded in formal trust frameworks. The Data (Use and Access) Act 2025 placed the digital verification service (DVS) trust framework on a statutory basis. Liability and accountability will also need to be clearly defined. For example, it should be clear who is responsible if a digital identity service (such as GOV.UK One Login or a commercial provider) fails. A failure could leave individuals or businesses unable to access a critical service or meet a legal obligation such as filing a tax return by the required deadline. Citizens' rights to transparency and official accountability could also be enshrined in law.

Clarity of purpose, scope and main objectives

4.13 Countries such as Denmark, Poland and France have implemented systems that support a wide range of uses, while in others, such as Sweden, private sector solutions are widely adopted. Systems with higher levels of adoption are associated with clearly defined use cases and integration into services.

4.14 Any future digital identity initiative would need to articulate the outcomes it is seeking, assess the alternative options available to achieve them and demonstrate why its chosen approach represents the best use of public money. This includes understanding the costs and risks of aligning existing systems and the implications of creating new dependencies or potential single points of failure.

Funding and responsibilities

4.15 Any future approach to digital identity is likely to involve significant direct and indirect costs. These will include costs associated with identity and authentication services, supporting technology and infrastructure, and arrangements for secure and trusted verification across public services.

4.16 There would also be consequential impacts on existing systems, data and processes. Public bodies would need to assess the costs of migrating from current authentication services and integrating digital identity across public services.

4.17 The costs and benefits of different approaches to digital identity will vary depending on choices about governance, delivery models and the respective roles of government and the private sector. Key considerations are likely to include:

- development, operation and maintenance of shared identity and authentication capabilities;
- transition and integration costs for public bodies;
- provision of supporting infrastructure, standards and assurance services;
- incremental costs to departments to issue verifiable credentials alongside existing physical documentation;
- impacts on devolved administrations and existing services, such as ScotAccount;
- administrative burden on individuals and businesses;
- how costs will be funded across central and wider government; and
- the implications for private sector organisations involved in providing identity and verification services.

4.18 Delivering digital identity requires coordination across multiple departments, public bodies and private providers. Future decisions will need to address the questions around who will lead on what, who will fund it and from where, who is accountable, and mechanisms for resolving issues between departments and between government and the private sector.

Data management

4.19 Successful identity schemes are supported by secure, effective access to and use of data across the public and private sectors. However, siloed systems continue to complicate data access and management in the UK, despite long-standing efforts to address these issues. Previous initiatives to standardise data and improve access, including enabling citizens to control their own data, have not yet delivered their intended outcomes. As previously reported, any future initiative would need to overcome the challenges and manage the costs of maintaining cross-departmental data in a good quality and usable form to ensure the effective ongoing operation of any joined-up systems after implementation.

Security, privacy and fraud

4.20 Well-designed systems can strengthen security and reduce fraud through privacy-aware approaches, such as data minimisation and improved anomaly detection. However, poor design choices could increase risks and reduce resilience. Any future initiative would need to set out how security and privacy will be integrated by design across legislation, policy, standards, procurement and delivery.

Compliance and adoption across the public sector

4.21 The UK has often faced challenges in aligning public sector organisations behind centrally led digital initiatives. There have been successes with the GOV.UK website and the GOV.UK Notify service, which allows public sector organisations to send emails, text messages and letters. However, digital identity presents more complex integration challenges because of variations in organisations' existing legislative and regulatory environments, processes, systems and data.

Clarity on the roles of public and private sectors

4.22 Evidence from countries such as Sweden suggests that widespread take-up can be achieved where identity services build on trusted, widely used providers and are reusable across public and private services. Successful digital identity will require clearly defined and understood roles for the public and private sectors, including how public services interact with certified providers. Any future approach would need to ensure consistency and interoperability so that individuals can easily use a certified digital ID across sectors and services.

International developments and standards

4.23 The use of international standards will support strong security and privacy and enable interoperability beyond the UK. The European Union Digital Identity (EUDI) initiative is a significant development, introducing an EU-wide secure digital wallet based on World Wide Web Consortium (W3C) verifiable credentials. The government has committed to using these standards and is testing mobile driving licences but has not yet set out whether UK digital identity solutions will interoperate with international systems such as EUDI wallets.

Stakeholder engagement and building trust

4.24 The UK's existing approach to digital identity is not yet well understood among its many stakeholders. Clear communications to explain objectives and address any conflicting priorities would be an important factor in building trust. Sustained engagement with citizens, businesses, providers and devolved administrations would also be essential.

Appendix One

Our audit approach

Our scope

1 This insights report considers the government's emerging approach to digital identity and the factors likely to influence its ability to deliver value for money. It focuses on the purpose and scope of digital identity; the respective roles of public and private sectors; lessons from previous UK initiatives and international experience; and the key design, delivery and governance issues that the government will need to address in any future digital identity initiative.

2 The report does not seek to evaluate the performance of individual digital identity products or services, nor does it assess the operational effectiveness of specific programmes. Instead, it provides evidence-informed insights to help inform policy choices, clarify trade-offs and highlight risks for consideration in any future decisions.

Our evidence base

3 Our evidence base comprised the following.

- Qualitative interviews with a range of stakeholders. These included central government policy leads (Cabinet Office and the Office for Digital Identities and Attributes), delivery bodies (Government Digital Service, Home Office) and public sector organisations operating identity and authentication services (Department for Work & Pensions). Stakeholders were selected to capture a range of institutional roles and viewpoints, rather than to provide a representative sample.
- Desk-based review of documents, including legislation, policy statements, consultation documents, standards and technical guidance and previous NAO work.

- Review of relevant international materials requested from the Supreme Audit Institutions of the following countries: Australia, Canada, Denmark, Estonia, France, Germany, India, Latvia, Lithuania, Norway, Singapore and Sweden.
- Use of published data and secondary research, including official statistics and sectoral analyses, to provide factual context on scale, adoption and market characteristics. Quantitative data are used descriptively and are clearly distinguished from qualitative findings.

4 The insights presented in this report reflect a synthesis of qualitative evidence, informed by documentary analysis and contextual data.

Appendix Two

Aspects of a coordinated identity system

1 **Figure 14** on pages 41 and 42 summarises the current UK position against the aspects of a coordinated identity system as set out in Part Four.

Figure 14
Aspects of a coordinated identity system

Any future approach to digital identity will need to address a range of factors to achieve value for money

Feature	Explanation	UK status
Legal and policy framework	Provides clarity on the scope and statutory basis for digital identity, ensuring consistency and trust in understanding and usage across both public and private sectors.	The UK has established the Digital Verification Services Trust Framework as a legally backed standard, requiring identity providers and services to be certified against it for use in specific regulated sectors.
Clarity of purpose and scope/use case	Clear outcomes and compelling use cases for individuals and businesses underpin successful take-up and utilisation. Benefits often arise from support for related aspects such as electronic signatures and simplified processes.	The UK has defined a limited set of use cases, most notably mandatory right to work checks, with other potential applications remaining optional or under development and dependent on wider adoption of certified providers.
Funding and responsibilities	Realistic and sustainable funding and resourcing would be needed both for the work directly required to support any future digital identity initiative (from legal and policy to technical) and for the related changes and investments needed for successful implementation.	No current proposals.
Data management	Successful identity schemes are combined with improved, secure access to and use of data across public and private sectors.	Long-standing fragmentation of UK public sector data systems continues to hinder effective data use.
Security, privacy and fraud	Digital identity initiatives are increasingly adopting W3C verifiable credentials to provide an internationally standardised, cryptographically secure, and privacy-preserving framework for asserting and verifying claims.	The UK has committed to using W3C verifiable credentials.
Inclusion	An increasingly digital state should not exclude those unable or unwilling to use digital channels, including non-UK-based individuals and non-UK residents or passport holders.	The UK intends to retain face-to-face and paper-based identity processes alongside digital options to ensure access for those unable or unwilling to use digital channels, including non-UK citizens.

Figure 14 *continued*
Aspects of a coordinated identity system

Feature	Explanation	UK status
Compliance and adoption across the public sector	Countries with successful digital ID schemes ensure they are implemented consistently across the public sector to deliver meaningful benefits to citizens, businesses and government alike.	The UK has historically found it difficult to achieve consistent public sector adoption of centrally led digital initiatives, and digital identity presents additional legislative and integration challenges.
Clarity on the roles of public and private sectors	Countries like Denmark, Poland and France have implemented systems that can be used for everything from online banking to single sign-in to public services. In some countries, private sector offerings, such as BankID in Sweden, are the most widely used.	Despite placing the trust framework on a legal footing, the UK's past mixed messaging on the role of private providers risks undermining investment, adoption and confidence in the digital identity ecosystem.
International developments and standards	Standards bodies, such as ICAO (passports) and ISO (driving licences) are complementing the foundational documents most often used for identity with their digital equivalents. The European Union Digital Identity (EUDI) initiative is also significant, implementing an EU-wide secure digital wallet based around W3C verifiable credentials.	The UK has committed to international standards such as W3C verifiable credentials but has not yet clarified the extent of interoperability with initiatives like the EU Digital Identity Wallet.
Stakeholder engagement and building trust	Clear and consistent communication and engagement would be an important consideration in building trust and encouraging take-up in any future approach to digital identity.	The UK's current digital identity approach is poorly understood, and inconsistent communication has raised concerns among providers and civil society that could impede trust and take-up.
Transparency and accountability	Countries cited as digital identity exemplars have embedded increased accountability and transparency into their laws and systems so that citizens can hold officials to account.	No current proposals.
Experience and usability	Digital identity needs to be well-designed and usable for both users and organisations.	No current proposals.

Source: National Audit Office assessment

This report has been printed on Pro Digital Silk and contains material sourced from responsibly managed and sustainable forests certified in accordance with the FSC (Forest Stewardship Council).

The wood pulp is totally recyclable and acid-free. Our printers also have full ISO 14001 environmental accreditation, which ensures that they have effective procedures in place to manage waste and practices that may affect the environment.

National Audit Office

Design and Production by NAO Communications Team
DP Ref: 017952-001

£10.00
ISBN: 978-1-78604-692-5