Cabinet Office

Making public services work for you with your digital identity

CP 1498

Government of the United Kingdom

Cabinet Office

Making public services work for you with your digital identity

Presented to Parliament
by the Chief Secretary to the Prime Minister at the Cabinet Office
by Command of His Majesty

March 2026

CP 1498

This publication is available at www.gov.uk/official-documents.

Any enquiries regarding this publication should be sent to us at publiccorrespondence@cabinetoffice.gov.uk.

Alternative format versions of this report are available on request from: www.gov.uk/guidance/contact-the-cabinet-office.

ISBN 978-1-5286-6190-4

E03528850 03/26

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by Cabinet Office

Contents

Ministerial foreword

Currently, it's too hard to get what you need from the government, when you need it.

The current legacy system of call centres, paperwork and the need to tell your story multiple times to different parts of government, with hours on hold and not knowing where you are in the process, is not good enough.

In its place, we will build a truly modern Britain where public services work for you.

A new digital state – that will be there for you when you need it most.

But first, we need to build the foundations for these new modern public services.

That's what the digital ID system is for.

It will be free to access for anyone who wants it and it will be built on three core principles:

- **It must be useful**: It needs to be easier than the old telephone and paper-based system.
- **It must be secure**: You will have more control over what data you share and we expect nothing less than banking levels of security.
- **It must be for everyone**: We won't leave people behind and will help you if you struggle with technology or don't have other forms of ID, like a passport, for example.

With digital ID, you'll be able to login to the GOV.UK App and prove who you are. But unlike an ordinary login, digital ID will work across different departments and come together in the GOV.UK App on your phone – so you can access all of the services you need in one place.

We know there's been a significant level of public interest in the digital ID system, which is why we're launching this national conversation, so you can have your say on how it is built.

This consultation seeks your feedback on how to build a system that is useful for everyone, to help you access the services you need.

For example, what information could be useful to include in the new digital proof of identity to stop the rummage for a utility bill or bank statement? Which government services could be improved? Like getting a driving licence or checking your tax code? And how will we make sure everyone is included?

Our baseline is to start with the fewest data points possible, enough to simply prove you are who you say you are and nothing more – but if more is needed to support the uses you and other members of the public want, like proving your address, that's something we'll explore.

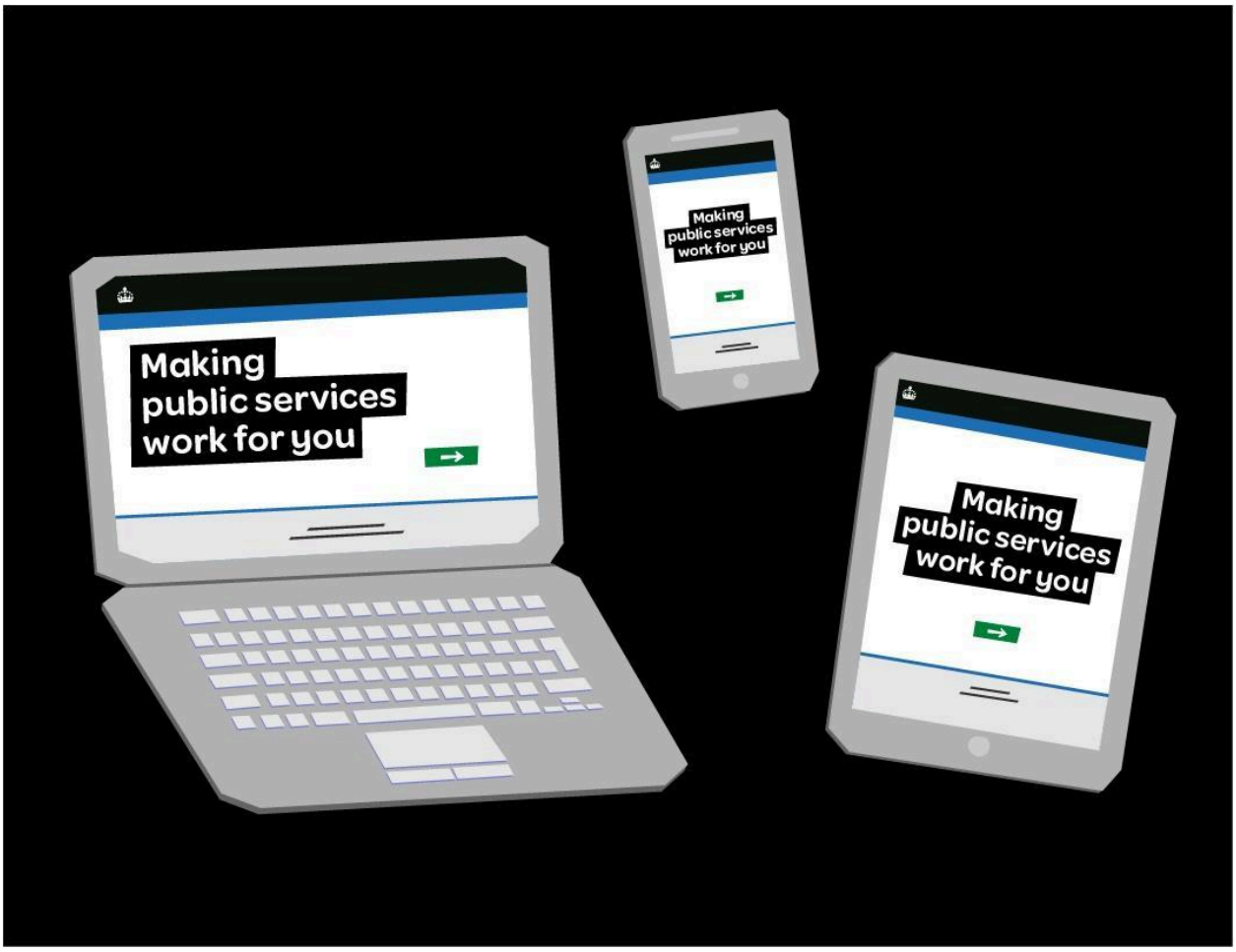
We cannot continue on this two-track approach where services in the private sector are fast, easy and digital and those in the public sector are slow, clunky and disjointed.

This is why this government is doing the hard work to build the foundations of the modern state and the public services of the future.

The digital ID system will help transform public services but we want you to want it and be part of it.

Now is your chance.

Rt Hon Darren Jones MP
Chief Secretary to the Prime Minister



Executive summary

The government intends to introduce a national digital ID (identity document) system. This will sit at the heart of next-generation digital public services in the UK and support innovation in the wider economy. It will help unlock entirely new ways to offer goods and services, and be key to making people's interactions with the state as efficient and useful as those they are accustomed to in the private sector, like online banking.

At its heart, this system is about making people's everyday lives easier by modernising old-fashioned processes. The new digital ID will:

- be a convenient way for people to prove who they are
- be secure and put people more in control of their data
- offer everyone eligible access to an inclusive ID, without up-front charges
- help government to reduce bureaucracy and build the intuitive, efficient, and responsive public services the UK deserves

We want people in the UK to shape the system and how it will work to ensure these objectives can be achieved. This is why we are running a wide-reaching and inclusive consultation to gather views and bring people together for discussion and debate, ultimately informing our future design choices.

We propose that three core principles will guide the design of the new digital ID. It must be:

- **Useful**: widely usable across the economy as a way for individuals to prove their identity – and central to the next generation of public services
- **Inclusive:** available to create and access at no cost to individuals and inclusive by design – helping those who currently struggle to prove who they are or are digitally excluded
- **Trusted:** underpinned by robust privacy, resilience and security measures that put people in control – built to rigorous government standards for digital verification services

We are designing the new digital ID as something people will want to get, rather than something they must have. There will be no legal obligation for people to have or present the digital ID.

The digital ID will primarily be stored as a digital document on someone's device, such as compatible smartphone or tablet. We expect it to include their full name, date of birth, a photo and nationality – though not all of this information will need to be shared in full when the digital ID is used. For example, where possible it will just share that a person is 'over-18' or has a right to work, rather than sharing their full date of birth or nationality.

To deliver the new system in the most cost-effective way possible, we will be expanding on existing government systems which are already successfully proving and verifying people's identities.

This consultation is structured as follows:

- **Part 1: Our ambition** introduces the current landscape before setting out our goals for the new system and the high-level benefits it will bring to people across the UK
- **Part 2: Our approach** describes how we are intending to build the digital ID system, harnessing the government's existing investments in developing a digital state. It explains the lifecycle of the digital ID – how it will be issued, where it will be stored and how it can be shared and checked
- **Part 3: Useful** discusses how the digital ID system has the potential to help us consistently identify people, so we can reduce bureaucracy and build more intuitive, efficient, and responsive public services in the future. It explains how it will be usable in the wider economy, and how we will make use of the digital ID to

help tackle illegal working, so that only those with the right to work in the UK can do so. These chapters ask questions about what information should be included on the digital ID and how it could be most useful to you

- **Part 4: Inclusive** covers the government's plans for an ID and digital inclusion drive, to make the digital ID available and accessible to all. It discusses who will be eligible, including the minimum age for the digital ID. It invites views on what groups may need extra support, what their needs are and what alternative access routes could look like
- **Part 5: Trusted** includes information on how we will design the new system to ensure that everyone can have confidence that it will protect their data. It includes discussion of technical security measures, data protection standards and how people can exercise greater consent and control when using the digital ID. There is also a chapter on governance and oversight
- **Part 6: Wider considerations** outlines our early assessment of the potential impacts of the system and the value we believe it could have, from helping us build more intuitive, efficient, and responsive public services to reducing friction in the wider economy

A national digital ID system is vital public infrastructure for the digital age. We want to draw on the expertise and wisdom of a wide range of stakeholders, from businesses to trade unions, technologists and civil society, as well as leaders in the public and private sectors who can use the digital ID to improve services for people in the UK. Key design decisions will only be taken after this consultation, to build the best possible product for everyone. We are grateful to everyone who takes the time to participate.

How to respond to this consultation

The consultation is open from 10 March to 5 May.

You can respond to the consultation questions via this survey link: http://www.gov.uk/government/consultations/making-public-services-work-for-you-with-your-digital-identity.

Alternatively, you can send responses to consultation@digitalid.cabinetoffice.gov.uk.

You will receive an automated email confirmation if your email response is successfully received.

Responses can be sent by post to:

c/o Digital ID

Cabinet Office

70 Whitehall

London

SW1A 2AS

When responding, please state whether you are responding as an individual or representing the views of an organisation.

Your response will be most useful if it is framed in direct response to the questions posed, though further comments and evidence are also welcome.

You can find the privacy notice for this consultation here.

Following this initial 8-week consultation period, we will be running a 'People's Panel on Digital ID' – an in-depth deliberative engagement process with a broadly UK representative sample of 120 individuals to discuss the policy in detail. Individuals will be selected through sortition (civic lottery).

Participants will be invited to a series of in-person and online workshops where they will learn about the policy area through expert presentations and panel discussions. They will be supported by expert facilitators to consider diverse perspectives and weigh trade-offs before working towards a shared set of recommendations for government. This process will conclude on 21 June, which will be the end of the formal consultation process.

Part 1: Our ambition

In the UK, we lack a single, authoritative way to prove that we are who we say we are. Online and offline, public and private services frequently ask us to prove our identity, but we have to do so using a range of documents that were never intended to play this part – like passports, driving licences and utility bills. This generates needless bureaucracy and leaves many struggling to afford, find or assemble evidence of their identity in their interactions with government and in the wider economy.

This leads to several problems:

- **Proving identity is confusing, complex and burdensome** – people can find having to navigate different documents and paperwork for different purposes frustrating and repetitive, while government, businesses and other organisations must also juggle this complexity. This places unnecessary burdens on people and creates unnecessary cost and administration, undermining efficiency in both the public and private sectors.
- **Government cannot deliver the modern public services that many people expect** – not having a single proof of identity which allows public services to consistently refer to people hampers this government's ambition to make them easy to access, more joined-up and responsive to people's needs and entitlements. This prevents faster, more proactive and personalised digital transformation in the public sector, trapping people in rounds of bureaucracy.
- **Unnecessary data security risks are created** – in order to prove their identity, people must hand over substantial amounts of personal data; usually more than is necessary. Worse, organisations often store copies of physical documents used for identification, increasing the risks of data leaks and knock-on issues.
- **A core group of disadvantaged people face persistent exclusion** – Cabinet Office research shows that 1 in 10 people in England, Scotland and Wales do not hold an in-date and recognisable photo ID, and the Lloyds Bank 2023 Consumer Digital Index indicates around 25% struggle to use digital services online. The most trusted documents – like passports and driving licences – come with a cost to obtain, while a lack of digital skills and smartphone ownership can create further exclusion. This locks people out of society, and especially the benefits of digitalisation.
- **We are saddled with high levels of fraud** – relying on a variety of physical documents also leaves room for abuse. Between June 2024 and 2025, fraud accounted for 44% of crime in England and Wales, according to the Office for National Statistics. Fake or stolen driving licences and passports are used by criminals to circumvent identity checks, and over 118,000 identity fraud cases were reported to the National Fraud Database in the first half of 2025. This costs people and organisations time and money to correct when things go wrong.

Proving identity digitally

Evidence suggests there is a better way to do identity verification. Digital identity documents ('IDs') have clear advantages over paper-based alternatives – they can be safer, more secure and more convenient. For instance, digital anti-fraud and security checks can provide greater confidence that someone is who they say they are. And, if someone's device is stolen, they can protect, lock and wipe it remotely. This helps keep people's information safe and makes it harder for criminals to misuse identities that do not belong to them.

A digital ID system also helps unlock entirely new ways to offer goods and services, such as the intuitive, efficient, and responsive public services the UK deserves. An authoritative understanding of someone's identity must underpin this work, giving public services confidence in who they are dealing with and the means to support people across departmental siloes. With this key building block in place, public services could better work for individuals, moving away from old-fashioned and bureaucratic processes, towards proactive, hassle-free services that are delivered when people need them and in ways that work for them. For example, when changing their name, someone could tell us once – with the change automatically updated across government services, without needing to tell departments one by one.

People across the EU and the rest of the world are already enjoying the many benefits of digital identities:

- **In Australia**, people can use their digital ID to access over 246 government services alongside a range of private services, from banking to buying alcohol. This reduces the need for multiple separate accounts and pieces of paper
- **In Denmark**, 97% of residents over the age of 15 use the national digital ID system, transforming their daily lives. For example, students can log in and automatically retrieve their education records and qualifications in job and university applications
- **In Estonia**, digital signatures enabled by the digital ID system are estimated to save the nation 2% of its entire economic output annually. The system also saves people time and effort, meaning they never have to provide the same information to government twice

However, progress in the UK has been slower. Within government, initiatives like GOV.UK One Login and the GOV.UK Wallet are beginning to revolutionise how people access online public services – providing a single 'front door' to government and allowing people to store secure digital documents instead of paper. In the private sector, digital verification service (DVS) providers operating under the Data (Use and Access) Act 2025, are also popularising digital identities. But, in many scenarios, how we prove and demonstrate our identity in the UK is still too burdensome, complex and outdated,

with many people unable to benefit from a DVS. Without government providing a foundational digital ID, many in the UK will continue to rely on paper-based documents, especially those who face ID or digital exclusion.

If the UK is to fully realise the benefits of digital identities, we must ensure that everyone can access a secure digital ID, and that they are supported to do so. To keep pace with the private sector and be a world leader in digital public services, we must modernise our approach to identification, using the best of technology to ensure everyone in the UK can access the public and private services they need, when they need them.

Chapter 1.1: Our proposed solution

To realise these benefits in the widest possible range of scenarios, the government has committed to creating a new national digital ID that will be useful, inclusive and trusted.

Above all, the digital ID will be useful. It will help people to prove who they are and things about themselves, like their age, in the public and private sectors. It will enable them to access a range of services more easily, better safeguard their information and privacy and give them more control over how their data is handled by others. If trusted by the public and widely adopted, this will save time, reduce duplication and create a basis for future innovation, driving down traditional forms of fraud.

The digital ID system will also be inclusive. For the first time, a digital identity solution will be freely available for all eligible British and Irish citizens and foreign nationals with permission to be in the UK. As part of the system, we will launch an inclusion programme. This will also help ensure those who do not have a compatible device, such as a smartphone or tablet, are less digitally confident or face particular challenges – such as those without permanent addresses – are not excluded. This will include looking at alternative access routes, such as physical products that still facilitate digital checks and in-person support, as well as the ability to have trusted individuals (e.g. carers, parents) act Wal of others.

Finally, the digital ID will be trusted. Experts at the National Cyber Security Centre will provide advice on its design from the outset. Core principles, such as data minimisation, will be built in from the beginning, and the solution will build on existing secure infrastructure, including the passport service, the eVisa service, GOV.UK One Login and the GOV.UK Wallet. This means the new digital ID will be saved securely on a person’s phone, putting them in control of that information, with most government data staying where it is already safely stored, in government departments.

Chapter 1.2: What the digital ID means for you

The range of ways people can choose to use their digital ID will grow over time. Early on, we expect it will be usable for simple things in the private sector, like proving age when purchasing alcohol. In these use cases, people will also be able to continue using any other alternatives they already use if they prefer – there will be no requirement to use the new digital ID.

Access to public services will not be made dependent on having the digital ID. However, for those who choose to take part, the digital ID system will provide a simple access point for new, modern digital public services, deepening and accelerating the work GOV.UK One Login is already doing. By providing everyone eligible with a trusted digital identity, which will support government to match and verify existing information about people across multiple public services in responsible, privacy-enhancing ways, it will be possible to deliver the services they need more quickly and effectively – without creating a single database of all government data about a person. This will also support the delivery of more proactive public services, meaning people could be able to automatically get the support to which they are entitled in a personalised way.

Another early priority for the digital ID system will be to support further efforts to tackle illegal working. Those who work in the UK without the right to do so undermine those who play fairly by the rules. By the end of this Parliament, the digital ID will therefore have a central role in the UK's right to work regime.

All employers in the UK already have a responsibility to prevent illegal working. Currently, they can do this by conducting prescribed right to work checks before employing someone. As part of this consultation, we are proposing to legislate so that evidence must be checked digitally as part of a prescribed right to work check. The evidence which can be checked by a robust digital process will include the digital ID, alongside British and Irish biometric passports (and Irish passport cards) and eVisas. This will be the only way for a business to demonstrate that they have carried out a right to work check to prevent illegal working.

The move to digital checking against this narrowed range of evidence will simplify compliance for individuals and businesses. For individuals, it will be easier to demonstrate a right to work, while it will streamline the recruitment process for businesses and create a digital audit trail of where checks have been carried out to support enforcement. Removing reliance on paper documents will also make it harder for criminals to use forged documents to gain employment and prevent unscrupulous employers from turning a blind eye to questionable documentation, helping ensure fairness in the labour market.

Chapter 1.3: Next steps

We intend for the digital ID to be available to those who want one by the end of this Parliament, following the necessary technical build and Parliamentary approval for the underpinning legislative changes. Further benefits will follow as the system helps us to enable the streamlined, digital, lifelong public service provision that people expect from government.

The digital ID system will only be a success if people trust it. This trust will only be built if they have a genuine opportunity to shape the system, which is why we have decided to take a new approach to this consultation that goes beyond simply asking for comments on proposals. We will ensure we make targeted efforts to involve those who may be most affected by the proposals, along with including those whose voices are often missing from more traditional consultations because of digital exclusion or other systemic barriers.

This exercise will be conducted in two stages. The first will involve 8 weeks of open engagement – running from 10 March to 5 May – where anyone who wants to take part can share their views. Alongside an online engagement platform, we will support local conversations and events across the UK. This includes roadshows, roundtables, as well as resources to help communities run their own discussions in ways that work for them.

In the second stage, which will follow the open engagement, we will bring together a broadly representative group of 100-120 people from across the UK to take part in a ‘People’s Panel on Digital ID’ – an in-depth deliberative engagement process. This group will hear views shared during the open engagement stage, discuss different perspectives, and openly debate areas of disagreement. We will support them to work together to weigh the trade-offs involved, explore common ground and develop shared recommendations for government. This group will not make decisions, but their recommendations – shaped by views shared in the open engagement phase – will help to inform next steps.

Together, these two stages will create an open and inclusive way for the public to be involved in shaping decisions about the digital ID system. We will also continue to engage with expert stakeholders throughout the duration of the consultation and beyond.

Views shared in both these stages will be carefully considered by the government to develop next steps for the digital ID system. A formal government response to the consultation will be published once all stages of the consultation have concluded and all responses have been properly considered.

You can find more information about the consultation and how to get involved in the two stages on GOV.UK. You can also access the full text in a range of accessible formats.

Questions on Part 1: Our Ambition

1.0.Q1. What do you think the main benefits will be, if any, for the government's new national digital ID system?

1.0.Q2. What do you think the main drawbacks will be, if any, for the government's new national digital ID system?

1.0.Q3. One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why?

a. Strongly Agree
b. Somewhat Agree
c. Neither agree nor disagree
d. Somewhat Disagree
e. Strongly Disagree
f. Don't know
    i. 1.0.Q3.1 Please explain your answer

1.0. Q.4 The government proposes to use the digital ID system to enable more modern, efficient and personalised public services. Which public services would you want the government to prioritise making faster or more efficient using the system?

Part 2: Our approach

Introduction

As set out above, the government intends to create a national digital ID that will be useful, inclusive and trusted. To support informed discussion of how the digital ID system could work in practice, this consultation begins by outlining our approach to creating, storing and using the digital ID. While final design decisions have not yet been made, this explanation will be vital for engaging meaningfully with the remainder of the consultation.

Chapter 2.1: Creating the digital ID

Building on existing infrastructure

In January 2025, we set out our diagnosis of the problems the government faces with digital technology in the *State of Digital Government Review*. This was accompanied by our plan of action in the *Blueprint for Modern Digital Government*, which this year's *Roadmap for Modern Digital Government* has put into motion. As part of the six-point plan for government digital reform, we have committed to strengthen and extend our digital and data public infrastructure and join up public services. This means improving the interface between people, the government and public services through the use of technology. Being able to prove your identity quickly and securely through the digital ID system is key to delivering on this vision.

Where possible, the digital ID will build on existing systems that are already operating as trusted parts of government. This infrastructure will be expanded and improved to meet the increased demands of the digital ID system and to bring its benefits to people sooner – leveraging the expertise that has already gone into creating secure and accessible digital solutions.

The four most relevant existing services are:

- **GOV.UK One Login** allows people to prove their identity once before using that digital identity to access more than 122 services across government. It is being rolled out across all central government services to replace the previous landscape of siloed and duplicate sign-in methods for public services. All government services are due to be onboarded by the end of 2027
- **The GOV.UK Wallet** enables GOV.UK One Login users to store and present digital versions of government-issued documents on their phones. This includes the Veteran Card and soon to be introduced Digital Driving Licence. It provides

users with greater security when sharing government documents, and gives users more control over what information they share when proving things about themselves, like age or identity

- **The passport service,** which is administered by HM Passport Office, part of the Home Office. HM Passport Office is the sole issuer of UK passports and is an authoritative source for information about nationality for British citizens
- **The eVisa service**, which is administered by UK Visas and Immigration (UKVI), part of the Home Office. eVisas are the authoritative source for identity and information about immigration status for foreign nationals in the UK, and have largely replaced physical immigration documents (such as biometric residence permits). This improves efficiency for service providers and increases security and fraud prevention, helping to deliver a modern border and immigration system

Additionally, an infrastructure for the trusted creation and use of digital identities already exists, including the *UK digital identity and attributes trust framework* (the 'trust framework'). This is a statutory framework of standards, rules and best practice that government publishes to show what a good digital verification service (DVS) looks like, against which a DVS can be independently certified. Certified DVS providers can apply to have their services appear in the statutory *register of digital identity and attribute services*, maintained on GOV.UK. This infrastructure helps people and organisations to find a trustworthy DVS. We intend for the national digital ID to operate within this ecosystem. We expect the GOV.UK Wallet (which will hold the digital ID) to be certified as a DVS, and GOV.UK One Login (as the umbrella service) will seek to maintain its certification against the trust framework.

Underpinning the digital ID in law

Unlike other digital versions of government-issued documents, like the forthcoming Digital Driving Licence, the digital ID will have no direct historical precursor. The government will be issuing eligible applicants with a new digital document, explicitly meant to serve as a standalone and authoritative proof of identity. We intend to legislate and ensure Parliamentary scrutiny of new measures to:

- create and issue the digital ID
- administer relevant identity and eligibility information on an ongoing basis
- manage the digital ID throughout its lifecycle (for more information on storing, managing and using the digital ID, see Chapter 2.2)

Issuing the digital ID

In general terms, issuance will proceed via the following steps:

- An individual will apply online for the digital ID, prompting them to login or create an account with GOV.UK One Login

- The individual may need to verify their identity (if they have not sufficiently done so previously) and will need to prove their eligibility for the digital ID. This will depend on what evidence they can present, leading them down one of the following routes:
    - If they can verify their identity using a UK passport or eVisa, their information is automatically checked with the authoritative source (HM Passport Office or UKVI)
    - If they are a British citizen and do not have a UK passport, they will be directed to a service that will inclusively support them to prove their identity and nationality (similar to HM Passport Office's first adult passport service)
    - If they are an Irish citizen, or cannot follow one of the above routes, they will need to provide appropriate evidence of their identity and nationality. As outlined below, this will take account of the arrangements of the Common Travel Area (CTA) as well as the rights recognised under the Good Friday Agreement
- On successful verification of their identity and/or eligibility, the government will issue the individual with a digital ID, tied to their GOV.UK One Login account

The digital ID will primarily be issued to people in a digitally protected format – known as a 'verifiable credential' – that can be stored on a device, such as a compatible smartphone or tablet. This will be similar to how people already store digital payment cards and tickets. Key considerations for the standards it will be built to will include:

- security
- widespread acceptance across a range of businesses and organisations
- potential for interoperability (within the UK, Common Travel Area and abroad)
- support for privacy-enhancing technologies like selective disclosure

Box 2.1.1. What is a verifiable credential?

Verifiable credentials are digital documents. Like physical documents, people can use verifiable credentials to confirm their eligibility to perform specific activities or verify claims about themselves. They typically contain information about the person they belong to, such as their name and photograph. As they are secured and presented via technical means, verifiable credentials can also be confirmed as genuine when they are used – for instance, proving they have been issued by an authoritative body like a government department, and have not been faked, tampered with or revoked.

In addition to this standard route, we are also considering whether alternative routes to accessing the digital ID will be needed, to ensure that all eligible individuals can access the system. More details can be found in Part 4, on making the digital ID inclusive.

Devolved and Common Travel Area considerations

We want to ensure that all British and Irish citizens, and people with permission to be in the UK, can use and benefit from the digital ID. We are committed to working with the devolved governments to ensure that the digital ID system will work effectively across the whole UK, recognising that many of the services where citizens could benefit from the use of digital ID are devolved matters, which are the responsibility of the devolved governments.

The introduction of this new system will take account of the arrangements under the Common Travel Area (CTA) as well as the rights afforded to people under the Good Friday Agreement.

In this regard, we respect the right of the people of Northern Ireland under the Good Friday Agreement to identify as Irish, British, or both, and to hold British and/or Irish citizenship without differential treatment. There will be no requirement that Irish nationals take British citizenship in order to benefit from the digital ID system.

We will also respect the arrangements under the CTA between the UK, the Crown Dependencies (Bailiwick of Jersey, Bailiwick of Guernsey and the Isle of Man) and Ireland.

British and Irish citizens will continue to be allowed to move freely, as now, to reside in either jurisdiction, and to enjoy associated rights and privileges including the right to work, study and vote in elections, as well as to access social welfare benefits and health services. The rights of cross-border workers, who live in Ireland and work in Northern Ireland or Great Britain and then return home (or vice versa), will be carefully considered.

The Government will continue to work with the Northern Ireland Executive, the Welsh Government, the Scottish Government, the Crown Dependencies, and the Government of Ireland with the aim of ensuring the digital ID system is developed in line with the commitments outlined above. The Government will continue to discuss those aspects of its digital ID proposals, which the Irish Government has an interest in, to ensure that they are compatible with existing legal obligations and the long-standing arrangements between both countries.

Questions about Chapter 2.1: Creating the digital ID

These questions are for experts speaking in their own capacity and for organisations:

2.1.Q1. The national digital ID will be issued as a credential (or digital document) for storage on a compatible device, similar to how people already store payment cards and tickets on their smartphones. Are there technical issuance standards, beyond those already used by the GOV.UK Wallet, that we should be building the national digital ID to?

a. Yes
b. No
c. Don't know
    i. 2.1.Q1.1. Please explain your answer and provide examples of the technical standards that should be used.

This question is for everyone:

2.1.Q2. Do you have any concerns about the impact of the national digital ID that are specific to your part of the UK? If so, please select which country and why?

a. Northern Ireland
    i. 2.1.Q2.1. Please explain your answer
b. Scotland
    i. 2.1.Q2.2. Please explain your answer
c. Wales
    i. 2.1.Q2.3. Please explain your answer
d. England
    i. 2.1.Q.2.4. Please explain your answer
e. No impact
f. Don't know

Chapter 2.2: Storing, managing and using the digital ID

Storing the digital ID

While all users will have the choice to store their digital ID in their GOV.UK Wallet, we are open to exploring whether and how it could be made accessible through digital verification service (DVS) providers, including via storage in third-party holder (often referred to as 'digital wallet') services. Our main objective is that any storage and use of the digital ID is secure, with only the entitled user able to access and use it.

Digital verification services

It could be possible for an individual to store their national digital ID in third-party holder services, via either a direct download functionality or by sharing a copy from their GOV.UK Wallet. People may already use holder services other than the GOV.UK Wallet and prefer these for a number of reasons, including perceived privacy benefits and preferences around user experience.

However, these benefits may be outweighed by reduced public understanding and reduced security, especially if information is improperly secured by third parties. For instance, in Chapter 5.3 we discuss how criminals could promote unofficial apps claiming to be the digital ID or GOV.UK Wallet to trick users into downloading malware or submitting sensitive data. Alternative holding solutions would therefore need to be at least as secure and resistant to fraud as the GOV.UK Wallet and not introduce weaknesses to the system. For this reason, we would only consider allowing a third-party to hold the national digital ID if certain conditions were met, including:

- It was certified as a 'holder service' under a current version of the UK digital identity and attributes trust framework, maintained by the Office for Digital Identities and Attributes (OfDIA) in the Department for Science, Innovation and Technology (DSIT)
- It appeared on the digital identity and attribute services register
- It had reached a specific agreement with government, including agreement to any necessary terms and conditions that may be informed by this consultation

Updating the digital ID

Some information held in the digital ID will be static, like a date of birth, assuming it has been correctly verified. Other information may change over time, like someone's name (if they get married or change it by deed poll) or their photo. However, in principle, any attribute about a person will need to be alterable, and their digital ID credential reissued, in case of errors in the issuance process. Each digital ID will also need to be updated or reissued periodically to accommodate technology changes or expiry dates. Further consideration of users' roles in keeping their digital ID up to date is in chapter 3.1.

Deleting and revoking the digital ID

Once issued, an individual may wish to delete their digital ID, or it may need to be revoked (i.e. cancelled), at a later date. For instance, someone might wish to remove their digital ID from their own GOV.UK Wallet. They will be able to do this at any time, and the process will be designed to be simple and quick.

When a user makes a deletion request, the digital ID will be permanently removed from their own device, and will no longer be usable unless they choose to redownload it. Relevant government departments will retain any relevant records that underpin the individual's digital ID in line with their data retention policies and privacy notices – much like how deleting an app does not automatically delete any account needed to use that app. This is necessary to meet legal and regulatory obligations, such as ensuring the security and integrity of the service and preventing fraud. Users will need to contact the relevant department directly if they wish to exercise their right to object to this processing. As we continue to join up public services through this system, we will explore how this process could be simplified.

The government will also need the power to revoke a person's digital ID in limited circumstances, such as if fraudulent usage is identified. Revocation will only occur in strictly controlled circumstances, and robust processes will be designed to govern revocation and other procedures. For more information, see Chapter 5.4 on Oversight and Governance.

Using and checking the digital ID

Once a digital ID has been created, people will need ways of reliably sharing it with those who need to check it, whether that is a public service, a business, charity or another person. These checkers, known as 'relying parties', need to have confidence that the data is accurate and has not been tampered with so that they can rely on it.

Unlike with physical documents, information on the digital ID should not be relied upon without being checked through technological means. This is because 'visual inspection' (i.e. where a person simply shows their digital ID on their device's screen to a relying party) could allow someone to show a faked or edited screen that human eyes cannot detect. Instead, the digital ID will need to undergo a technical check, via a process called 'programmatic verification,' whenever it is presented.

For instance, rather than someone just showing their digital ID to a shop assistant, they would present it from their GOV.UK Wallet to be scanned by the shop assistant. The assistant might use a device provided by their employer or a physical terminal, like a payment terminal used for contactless payments, to do this. This will help confirm that a digital ID has not been faked, tampered with or revoked.

Intermediary services

We expect most checking in the wider economy to be done by intermediary DVS providers – and remain committed to the model underpinned by the Data (Use and Access) Act 2025. To deliver on our goals of maintaining end-to-end security and trust, only DVS providers that are certified under a current version of the trust framework and present on the government register will be able to programmatically verify a digital ID presented from the GOV.UK Wallet, offering robust checks as a service to relying parties. Several such 'orchestration' services are already available from providers on the government register.

We expect DVS will want to provide a variety of checking services (with user agreement), such as:

- offering sophisticated checks which are suitable in commercial settings or regulated industries
- including functionality such as record keeping for auditing purposes
- integrating the digital ID into existing user journeys in the wider economy (such as payments journeys)

Separately, we intend for suitably certified and registered DVS providers to be able to build on the digital ID in the same way that we have discussed elsewhere for other credentials in the GOV.UK Wallet. For example, a DVS provider could use information from the national digital ID in the GOV.UK Wallet to create their own new digital credential, potentially combined with other information they have sourced. This is also known as a 'derived credential' which could be used to prove a range of different things about someone.

Government Checker service

We also intend to develop a 'Government Checker', which will support orchestration and credential verification. This service will support public sector relying parties to consume and trust credentials, including the national digital ID, in a range of scenarios. We intend for the Government Checker to be certified and registered as a DVS under the Data (Use and Access) Act 2025.

When someone presents their digital ID (or another credential) from their GOV.UK Wallet, the relying party checking the credential will be able to scan it using the Government Checker. The person whose GOV.UK Wallet it is will then be asked to approve sharing the requested information, before the relying party is likely to receive:

- confirmation that the presented digital ID is valid and trustworthy
- the key data for that use case, which could be limited so that only necessary information is shared (for instance, that the person is over 18, rather than sharing their full date of birth)

- a photo of the person to whom the digital ID belongs so they can confirm it is being presented by the right person

Given the importance of programmatic checking and robust data sharing for all transactions, we are also exploring whether a basic Government Checker service should be made available for free or at low cost to relying parties in the private and third sector. In these instances, we would envisage several limitations to the service by design. For instance, it would only verify government-issued credentials, not those made by private sector DVS, and could have other functionality or usage limits. This is because the Government Checker would not be meant for verification at-scale or use in most commercial settings. Outside of government, it would instead be intended to remove the risk of visual presentation in certain low-volume use cases. For instance, even if it was made widely available, we expect that companies conducting large numbers of right to work or age verification checks would be better served by third-party DVS providers providing a specialist service. We welcome views on this proposal.

Questions about Chapter 2.2: Storing, Managing and Using the digital ID

These questions are for everyone:

Someone might wish to delete their own digital ID from their device. They will be able to do this at any time, and the process will be designed to be simple and quick.

2.2.Q1. Are there any ethical factors government should consider that relate to an individual deleting their digital ID?

a. Yes

b. No

c. Don't know

    i. 2.2.Q1.1 Please explain your answer.

Under strictly controlled circumstances, the government may also have the power to revoke (i.e. cancel) someone's digital ID – for instance, if someone's digital ID has been identified as stolen or used fraudulently. This will be governed by robust processes.

2.2.Q2. Are there any ethical factors government should consider that relate to revoking (i.e. cancelling) an individual's digital ID?

a. Yes

b. No

c. Don't know

    i. 2.2.Q2.1 Please explain your answer.

2.2.Q3. Do you think people should be able to choose to store their national digital ID directly in holder services (sometimes known as 'digital wallets') other than the GOV.UK Wallet, that are certified to meet government standards?

a. Yes

b. No

c. Don't know

    i. 2.2.Q3.1. Please explain your answer.

These questions are for experts speaking in their own capacity or for organisations:

2.2.Q4. To support secure use, there needs to be a robust way to check the national digital ID presented from the GOV.UK Wallet. This will help confirm it has not been faked, tampered with or revoked. The private sector has already developed free and paid-for checking services. In addition, we are considering creating a 'government checker' service. To what extent do you agree or disagree with the proposed government checker service being made available for use in the private and third sectors, at low or no cost?

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don't know
    i. 2.2.Q4.1. Please explain your answer

2.2.Q5. We are considering several limitations to the government checker service, by design. For instance, it could only be able to check government-issued credentials, like the national digital ID. This is intended to leave room for third-party checking services. Are there any specific limitations you think we should set for the government checker?

a. Yes
b. No
c. Don't know
    i. 2.2.Q5.1. Please explain your answer

Part 3: Useful

Introduction

The national digital ID will be transformative for government services and sectors across the economy. Our aim is that the national digital ID will:

1. sit at the heart of next-generation public services
2. give people a foundational and trusted proof of identity for use across the economy
3. underpin a simpler and more secure model to prevent illegal working

The digital ID is being designed as something which people will want to have, rather than something they are forced to get. In all cases, our intention is that it will be acceptable alongside other suitable proofs and not replace other government-issued documents people might already have. For example, the digital ID will not assert entitlement to drive or entitlement to cross borders – which will continue to require a driving licence and passport, respectively. However, we expect it will, in time, reduce reliance on physical documents as people choose to apply for and use the digital ID.

How the digital ID can be used may also vary across the devolved governments of the UK. While immigration policy (and therefore right to work regulation) is reserved, so can be set centrally by the UK government, devolved governments can have different requirements for accessing and joining up public services, and for some use cases in the wider economy, such as acceptable proofs for age restricted goods. As outlined above, we will work with the Welsh Government, Northern Ireland Executive and Scottish Government to seek consistency and usefulness across the country.

Chapter 3.1: Information contained in the digital ID

For the digital ID to be useful in any given setting, it needs to be able to prove information relevant to that scenario. That information also needs to be trusted by the person or organisation checking it, and appropriate for the regulatory landscapes in which it operates.

However, no digital ID can, or should, be the definitive proof of every piece of information about an individual. The digital ID will therefore seek to strike a balance,

holding enough information to usefully prove identity information, without requiring unnecessary data collation or storage.

Core information about an individual

Each digital ID will contain core information about a person. We propose that this will include:

- full name (as it appears in official documentation like a passport)
- date of birth (which could be selectively disclosed in different ways, including as just an ‘over 18’ or ‘over-65’ attribute)
- nationality (which could be selectively disclosed in different ways, including as confirmation that someone has a right to work in the UK)
- a current, high-resolution biometric facial image that meets specified requirements

Box 3.1.1 Data minimisation and selective disclosure

Data minimisation is a privacy-preserving principle that encourages not collecting, sharing or otherwise processing more personal data than is necessary for a specific purpose. It is enshrined in the UK General Data Protection Regulation (UK GDPR).

While the principle is being applied to how the national digital ID is designed, created and managed, it also applies to how it is used. For example, the practice of ‘selective disclosure’ gives people specific control of what information they share, and with who. When someone shows their physical driving licence at a bar, they have no choice but to disclose all the information on it – including unnecessary attributes like full name and address – alongside relevant information like date of birth and a photo.

By contrast, the digital ID will go further in preserving privacy by minimising the data it discloses. For example, where possible it will just share basic information, such as that a person is ‘over-18’, rather than sharing their full date of birth. The digital ID is being built with this functionality in mind to help ensure no more personal data is shared than necessary when the digital ID is used.

In addition to this core identity information, the digital ID may also need to store and share additional information or metadata (i.e. data about information held). This could include:

- the level of confidence which government has in the individual’s identity, based on the evidence provided, to help relying parties understand if it meets their needs
- whether the person to whom the digital ID relates has an authorised representative acting with delegated authority on their behalf, such as through a power of attorney

- other information identified as necessary via this consultation or further policy development

We believe the information above will provide sufficient basis for the intended uses for the digital ID (see the remainder of this Part), without requiring any unnecessary information to be collected or shared.

Information to support joined-up public services

We are exploring what information is needed to better link public services. Currently, people in the UK have multiple identifiers, for example National Insurance numbers and passport numbers. This means we cannot know when it is the same person accessing different services. Without this, it is very difficult to match people across services so they can be delivered in a personalised and efficient way.

We are considering developing a universal unique identifier (or similar approach) tied to the digital ID and GOV.UK One Login, to enable consistent reference across government services. This will be key to delivering next-generation, digital public services in the UK. This identifier would not need to be visible or used outside the public sector, and we are exploring providing it only to those choosing to use the digital ID. More information can be found in Chapter 3.2 on Transforming Public Services.

Over time, such an approach could streamline information updates, ensuring verified changes are reflected across services and reducing the need for people to repeatedly provide core information. It could also support more proactive, personalised services. For example, if you update your name on the digital ID, this could be updated automatically across other connected government services. Any implementation would require appropriate legal gateways and robust privacy, security and transparency measures.

Consideration of further information

Address

Being able to prove current address through the digital ID could be a more efficient and easier option than relying on physical evidence, such as council tax bills and bank statements. If your digital ID were able to provide an authoritative proof of your current address, it could reduce friction and save you the burden of finding recent physical documents to prove this. It could also support public services where this information is relevant.

However, it is unclear how cost effective it would be for us to provide authoritative current address information on the digital ID, and the extent of the complexities involved. Existing documents, such as driving licences, ‘verify’ address by sending the document to the address provided. This is not an option for the digital ID and, as such it is difficult to be confident that a provided address is accurate and in use – for example,

in circumstances where someone might move addresses often. Developing a way to verify current address information to a sufficient level of confidence for it to be relied upon as a sole proof of address would therefore have implications on the cost and complexity of the system.

We are interested in further understanding the ways that verified current address information could be used and how the government could verify address information and keep it up to date, while not adding an extra burden on people who face exclusion.

Sex or gender information

In the UK, sex and gender data can cover three categories:

- **Biological sex**.
- **Legal or certified sex**. This is sex as recorded on your original birth certificate or as amended under the Gender Recognition Act 2004. In almost all cases, legal or certified sex reflects a person's biological sex.
- **Gender**. A broad term that is sometimes used interchangeably with sex or when specifically referring to social rather than biological differences between sexes. It can also capture data that equates to biological, legal or certified sex.

Information about sex and gender is not necessary for the intended purpose of the digital ID. Inclusion of this information would not enhance checks that the digital ID belongs to the person presenting it. Checks will be done programmatically and through biometric authentication, neither of which require specific sex or gender data.

Additionally, digital right to work checks and many checks in the private sector (including Know Your Customer (KYC) and simple age verification checks) do not require the collection or sharing of information about a person's sex or gender. Similarly, access to most public services does not require this information. In specific scenarios where sex or gender information is required, it is better collected and verified by other means appropriate to that scenario, rather than contained in the digital ID.

For these reasons, and in line with data minimisation principles, we do not intend to include sex or gender information in the digital ID.

Keeping details up to date

For the digital ID to be useful and trusted, it is important that the information it contains remains up to date. Changes to an individual's core identity information, such as name changes, can occur for legitimate reasons and are common.

We are exploring whether people should be legally required to inform the government, within a suitable timeframe, of any errors or changes to personal information held in their digital ID, so that it can be updated, and what an appropriate form of enforcement

could be. We are mindful that putting an obligation on users to keep their digital ID up to date may be unduly burdensome or disproportionate, especially for some groups with protected characteristics.

Questions about Chapter 3.1: Information contained in the digital ID

This question is for everyone:

3.1.Q1. The national digital ID will include a person's full name, date of birth, nationality, and a biometric facial image (photo). What further information, if any, should the digital ID also include?

This question is for organisations:

3.1.Q2. The government is not planning to initially include address information on the national digital ID, but we may review this position in the future. If your organisation were to rely on this information, what would help you trust an address on the digital ID?

This question is for everyone:

3.1.Q3. Businesses and organisations accepting the national digital ID need to trust that the information on it is up to date and accurate. We are exploring whether people with a digital ID should be legally required to inform the government within an appropriate timeframe of certain changes (such as a name change) or errors to their personal information, so that their digital ID can be updated.

To what extent do you agree or disagree with a legal requirement to inform the government of changes or errors within an appropriate timeframe?

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don't know
    i. 3.1.Q3.1. Please explain your answer

Chapter 3.2: Transforming public services

The national digital ID system is key to enabling streamlined, digital, lifelong public service provision. To be clear: access to public services will not be made dependent on having the digital ID. However, should people choose to get the digital ID, it will be possible to help reduce the time and effort they spend interacting with the state to access the services to which they are entitled. This is because identifying ourselves and proving our entitlements is the first step to many interactions with the public sector.

People will come into contact with public services many times over the course of a lifetime. Half of UK adults interact with government administrative services around once a year, according to research from the Office for National Statistics. These interactions are likely to be more frequent for people who need additional support. At the same time, people who need additional support can often be those who struggle the most to prove their identity using existing forms of evidence, like passports or driving licences (as outlined in Part 4 of this consultation, on being inclusive).

Below are some examples of why someone might need to interact with a public service and, in doing so, prove who they are or their entitlement to that service.

From birth, a parent or guardian may need to engage with the state numerous times to access essential services, including when:

- applying for a first passport
- checking a child's eligibility for or applying for help with childcare costs
- adding a child element to a Universal Credit account
- accessing emergency housing or financial support

As a young person, someone may need to engage with the state to access services such as:

- proving a right to work for their first job
- applying for or proving eligibility for a student loan
- accessing inclusion and digital access support for people not in education, employment or training (NEET) or the young people's services

Throughout adult life, after the age of 18, someone may need to:

- access Universal Credit
- apply for or renew a full driving licence
- register a marriage
- register as homeless or in need of housing support

Later in life, someone may need to:

- claim a state pension
- apply for or check eligibility for winter fuel payments or warm home discount
- apply for an older person's bus pass

- register a power of attorney

While proving identity is often the first step to accessing these services, in the UK this is too regularly an imperfect and inefficient process that relies on people finding and providing the right combinations of physical evidence. Additionally, because different government departments often work in siloes, people can feel like they are starting from scratch each time they interact with a different part of the public sector.

How digital ID can help

We want public services to be easily accessible throughout a person's life – whether that means a student using their digital ID to easily access services for themselves or a parent accessing services on behalf of their child. Our vision is to make people's interactions with the state as efficient and useful as possible, as is already the norm in areas of the wider economy, such as in online banking, and in other countries.

Below is an example of how Estonia has personalised child benefit administration by using a foundational digital identity to underpin modernised public services. This example is included for reference only – the national context in Estonia varies significantly to that of the UK. However, it still provides a useful illustration of what a national digital ID system could make possible.

Box 3.2.1: Case Study Streamlining Child Benefit Administration

When a child is born in Estonia, parents experience a seamless, digital-first system for accessing financial support. Using their digital identity, parents register the birth online within minutes. Immediately afterward, a tailored benefits offer appears in their government account. Parents simply review and accept the offer – no additional forms, uploads, or supporting documents are required.

Behind the scenes, eligibility checks continue automatically. Population and school records are linked to ensure that payments remain accurate and up to date until the child turns 18. Parents or guardians only need to report major changes, such as a new address, which can be done quickly through the same digital portal.

Estonia's example demonstrates how fully integrated, proactive digital services can reduce administrative burden for people while ensuring more accurate and responsive delivery of support. This stands in contrast to the experience people currently have across much of the UK. Parents, carers or guardians must usually determine their own eligibility via guidance found on GOV.UK, navigate multiple and sometimes complex application routes depending on their specific situation, and gather physical documents to evidence their claims. If their circumstances change, they often need to revisit this process from the beginning – rechecking eligibility, resubmitting documents, and repeating applications to different schemes.

Digital ID as the foundation of transformed public services

This government is committed to bringing public services into the twenty-first century. The digital ID system will be the cornerstone of this transformation – learning from successful systems around the world while keeping the UK government's values of privacy, transparency and inclusion front and centre. We expect the digital ID will help us to:

- remove persisting barriers to public services, like ID exclusion (see Part 4 on how the digital ID system will be inclusive)
- speed up service delivery by further eliminating repetitive and inefficient identification processes
- save taxpayers' money and lower costs to government by reducing reliance on paper-based identity documents, which can be more easily faked
- give people more control over how they interact with public services and how they prove their identity and eligibility

From the outset, the digital ID system will offer people a secure, inclusive and reusable credential that can be used across the public sector to prove their identity – the first step for proving eligibility for many public services. This will build on work that GOV.UK One Login is already doing to reduce duplication of identity processes across government. While applying for and using the digital ID will not be required to access public services, in time, we expect it will reduce reliance on physical documents as people choose to adopt it, while making processes easier and quicker than they are today.

In time, the digital ID system will also help enable modern, personalised and joined-up public services. A trusted digital identity will provide the foundation for government to deliver the services they need more quickly and effectively – without creating a single database of all government data about a person. Instead, this will support public services to match and verify existing information about the people they serve in responsible, privacy-enhancing ways – such as via a universal unique identifier (or similar approach). This means public services could better work for individuals, when they need them and in ways that work for them, letting government move away from old-fashioned and bureaucratic processes, towards proactive, hassle-free services that are available at the point of need.

How this will look and feel will evolve over the coming years, as we hear from people throughout the consultation and beyond. It will take time to fix the foundations of the digital state. However, below are three illustrative examples of how we envisage the digital ID system could help transform public services:

- **Enabling inclusion.** The digital ID system will reduce existing, systemic barriers to accessing public services. A free to access, digitally verifiable credential will help address traditional identity documents being financially or otherwise out of

reach for many people. For example, it will give people who do not already have one an authoritative proof of identity when applying for funded childcare schemes. This will help ensure people can access the services to which they are entitled

- **Saving people time.** The digital ID system could also help ensure that people no longer waste time proving to public sector organisations who they are or chasing the support they need. For instance, by underpinning a way to consistently reference people across government services, it could enable more proactive and personalised public service delivery. In the future, integration with national and local services could fundamentally reshape the interaction with individuals and communities, with a shift from impersonal processes to outcomes that meet the specific needs of individuals
- **Reducing fraud**. The digital ID system will lessen our reliance on insecure physical forms of evidence. When a service needs to verify something about a person, their devices will perform a secure digital 'handshake' using trusted technical standards. This will mean fewer photocopies of documents being stored or shared insecurely and safer interactions for people and the organisations they interact with. This will make it harder for criminals to exploit weaknesses, whether that be using fake documents or impersonating someone. This could free up government resources for inspecting other access routes more thoroughly

We recognise that these potential outcomes cannot be achieved without the support and cooperation of devolved governments, local authorities and other delivery partners who understand issues people face at the grassroot level. We are committed to working closely with these groups to help ensure that the benefits of the digital ID system are realised similarly across the length and breadth of the country.

Questions about Chapter 3.2: Transforming public services

These questions are for everyone:

3.2.Q1: We know that people can struggle to access or claim the public services to which they are entitled. We want to identify key issues in these interactions, so that we can explore how the digital ID system could help address these, making people's lives easier. When people are interacting with public services, some common issues could be:

- **Signposting** – people might not know what public services are available to them
- **Privacy concerns** – people might be concerned about who information about their situation will be shared with
- **Time and effort** – people might not find the time to complete the processes needed to access public services they are entitled to
- **Proving their identity/eligibility** – people might not have access to the required letters, documents, or reference numbers needed to check their eligibility for, or to, access public services

Are there examples of any barriers or inefficiencies that prevent you (or people you support) from interacting with public services, that you think the digital ID system could help with?

a. Yes

b. No

c. Don't know

    i. 3.2.Q1.1. Please explain your answer

3.2.Q2: Have you ever faced issues with knowing which public services are available to you based on your circumstances or, if you support other people, have you faced similar issues when supporting them?

a. Yes

b. No

c. Don't know

    i. 3.2.Q2.1. If YES, please explain your answer

3.2.Q3: Have you ever been unable to or had difficulty accessing a public service because you were unable to prove your identity or, if you support other people, have you faced similar issues when supporting them?

a. Yes
b. No
c. Don't know
    i. 3.2.Q3.1. Please explain your answer

3.2.Q4. For those who opt for a digital ID, government would develop a method to securely identify and match people across different public services to simplify everyday interactions between individuals and the state.

For instance, such an approach could help ensure changes in an individual's information are easily and quickly reflected across services, like a name change. This would reduce the need for people to update their information separately for each service. It could also let government move away from old-fashioned and bureaucratic processes, towards proactive, hassle-free services that are available at the point of need.

To what extent do you agree or disagree with the adoption of such an approach to public sector transformation?

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don't know
    i. 3.2.Q4.1. Please explain your answer

3.2.Q5. What ethical issues, if any, can you think of when designing a way to identify and match people across services?

This question is for experts speaking in their own capacity and organisations:

3.2.Q6. What technical issues do we need to think about when designing a way to correctly identify and match people across public services?

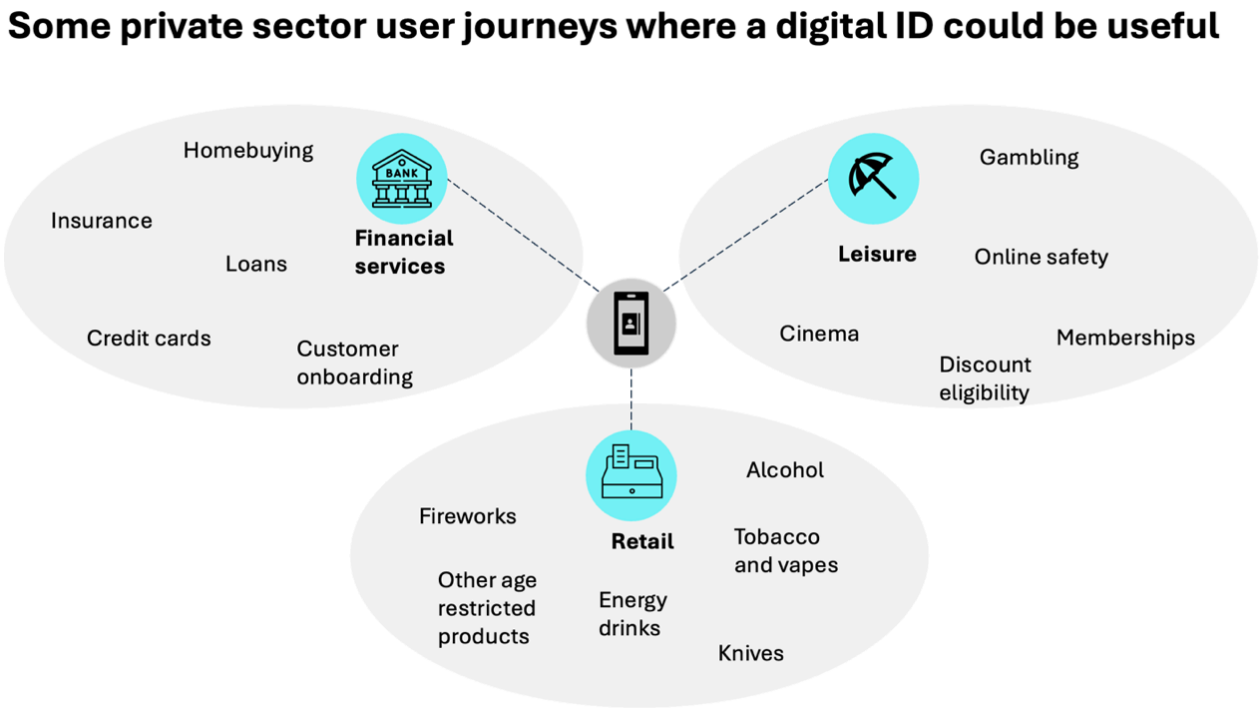
Chapter 3.3: Utility in the wider economy

While the national digital ID will not completely remove the need for individuals to collate other evidence and paperwork in some transactions, an inclusive, purpose-built and privacy-centric credential has the potential to revolutionise how people prove things about themselves in their daily lives.

In areas without specific regulatory requirements, there are unlikely to be inherent barriers to the use and acceptance of the digital ID. This includes situations such as proving who you are when collecting parcels or joining a gym. This means the digital ID could be useful for people in the short term across a range of different scenarios.

Across the economy, there are many other transactions where regulatory or other requirements mean an individual must present proof of identity or eligibility. This includes regular experiences, like buying a bottle of wine or visiting age-restricted websites, to more significant and infrequent occurrences like getting a mortgage.

Diagram 3.3.1 – Indicative age and identity use cases in the private sector where the digital ID could be acceptable



For the digital ID to be trusted and accepted across the economy, we will need to remove barriers to its use and create a framework of safeguards and operational requirements. Work is already underway to deliver many of the necessary changes in

regulated sectors, so that a digital verification service (DVS) can be used safely and securely, alongside physical documents. This includes:

- Ofcom has listed digital identity services as a potentially highly effective method of age assurance, with DVS certification one way to provide evidence of compliance
- the Home Office will update the alcohol mandatory licensing conditions to allow for age verification using registered DVS when buying alcohol
- the Tobacco and Vapes Bill will provide a regulation-making power, which will enable specific provision to be made to make clear how DVS can be used securely for tobacco and vape sales
- the Home Office intends to follow the same approach of providing a regulation-making power in the Crime and Policing Bill, to make clear how DVS can be used securely for the sale of knives and other bladed articles
- DSIT has worked with HM Treasury to jointly produce guidance on using digital identities for identity and Know Your Customer checks as required under the Money Laundering Regulations

As we expect the GOV.UK Wallet (which will hold the digital ID) to be certified as a DVS under the Data (Use and Access) Act 2025, these changes could pave the way for people to choose to use the digital ID across the economy. For instance, the digital ID could support the use of trustworthy electronic signatures, providing a way for people to prove their identity before digitally signing a document in the homebuying process.

These changes will also unlock opportunities for people to use other certified DVS providers and documents in the GOV.UK Wallet should they wish. Government remains committed to the work that is already ongoing to enable the use of digital verification services in a range of further scenarios, and to encourage the use of DVS for digital right to rent checks and Disclosure and Barring Service identity checks by those who would like to conduct a check digitally.

The government has also recently launched an evidence-led consultation on how to ensure children's experiences online are safe and enriching. The consultation asks about how children use digital technology, as well as potential new measures for keeping them safe online, and will be open until 26 May 2026. It includes questions about how age verification technologies, like the national digital ID, could support effective implementation of current and future protections.

Where appropriate, we are working across government and with regulators to ensure that where any digital identity, including the national digital ID, is accepted, it is done in a robust way – for instance with sector specific regulatory and legislative requirements for programmatic checking (see chapter 2.2). This is intended to prevent organisations from relying on insecure visual inspection methods.

In some cases, the relevant legislation, regulation or guidance which is necessary to enable acceptance of the digital ID may be devolved. We will work closely with the devolved governments and seek to secure legislative consent as necessary so that people across the UK can make the same choices about whether to use their digital ID in their daily lives.

Across all uses, the digital ID will be optional. It will give people more choice for how they operate in the economy and share their data, rather than becoming the *only* choice.

Questions about Chapter 3.3: Utility in the wider economy

This question is for everyone:

3.3.Q1. The national digital ID would be useable across the private and public sectors, alongside other options like physical documents and other appropriate digital identities from third parties.

To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?

a. Strongly agree
b. Somewhat agree
c. Neither agree nor disagree
d. Somewhat disagree
e. Strongly disagree
f. Don’t know
    i. 3.3.Q1.1. Please explain your answer

Chapter 3.4: Tackling illegal working

As part of the digital ID system, we are exploring changes to how right to work checks are conducted in the UK to more effectively tackle illegal working. Under UK legislation, access to work is reserved for those with a right to work. This includes British and Irish nationals, and those whose immigration status entitles them to work. All employers in the UK already have a responsibility to prevent illegal working by those individuals who are not entitled to do so.

An employer can check someone's right to work by conducting prescribed checks before employing someone. The checks apply irrespective of nationality and include British and Irish citizens. Conducting these checks ensures an individual is not disqualified from carrying out the work in question by reason of their immigration status. It also ensures businesses can obtain a statutory excuse (a defence) against liability for a civil penalty where illegal working is detected.

There are currently three main ways a business can complete a right to work check:

- A manual check of original documents from a prescribed list of accepted documents (all citizens)
- A digital check using a digital verification service (DVS) that offers Identity Document Validation Technology (valid British passport and Irish passport or Irish passport card holders only)
- A Home Office online check (non-British and non-Irish citizens with an eVisa only)

How right to work checks could change

Our ambition is that digital right to work checks will be mandatory by the end of this Parliament for the purpose of obtaining a statutory excuse. The evidence which can be checked by a robust digital process will include the digital ID (including any alternative access solutions), alongside a British/Irish passport (or Irish passport card) or an eVisa.

We are therefore proposing to legislate so that evidence must be checked digitally as part of a prescribed right to work check. Amendments will be made to the secondary legislation and statutory codes of practice to prescribe robust digital checks as the only acceptable means by which the above evidence can be checked and the statutory excuse obtained. We will also remove alternative forms of evidence deemed no longer valid to establish a statutory excuse, such as birth certificates, and set out within the code of practice how businesses can conduct digital checks using the narrowed range of evidence – including via an appropriate DVS.

The move to only digital checks will:

- make it easier for people to demonstrate their right to work by not having to find and potentially post original physical documents to prove their identity
- make unreliable manual checks of varied paper documents unacceptable, making it harder for criminals to use forged documents to gain employment and helping to mitigate fraud
- reduce the risk of people's data being misplaced or leaked by replacing copies of paper-based documents with secure digital checks
- create a digital audit trail of where checks have been carried out, helping businesses to demonstrate compliance and supporting enforcement
- minimise the data people share with businesses for right to work checks
- make it simpler and quicker for businesses to conduct checks, and therefore comply with government requirements, by standardising the process
- increase the accuracy of checks through automated validity checking and minimising the potential for human error

We recognise that some right to work checks may still need to be carried out via an exceptions handling process. This will be set out in the statutory codes of practice.

Business support

All businesses recruiting from the date of implementation of these changes will need to carry out a digital right to work check for new workers to obtain a statutory excuse against a civil penalty. This means that there will be no need to retrospectively carry out right to work checks for workers already in post.

The government is committed to ensuring that businesses are supported in the transition to digital right to work checks. We will therefore be implementing:

- a transition period between the introduction of the digital ID for individuals and mandating digital right to work checks to obtain a statutory excuse
- a communications campaign and business engagement
- business training to support the move to exclusively digital checks

As set out in Chapter 2.2, we are also considering whether the government should make available a free or low-cost checker service, known as the 'Government Checker', to support checks of the digital ID.

Questions about Chapter 3.4: Tackling illegal working

As a reminder: please do not include information that could identify a specific individual in any free text responses.

These questions are for everyone:

3.4.Q1. Are there any additional challenges not captured in the consultation that businesses would face in carrying out fully digital right to work checks for all new workers?

a. Yes

b. No

    i. 3.4.Q1.1. Please explain your answer

3.4.Q2. Would any additional support not captured in the consultation be required for business to comply with fully digital right to work checks?

a. Yes

b. No

    i. 3.4.Q2.1. Please explain your answer

This question is for organisations:

3.4.Q3. What information would your organisation require to have confidence that a digital right to work check has been completed?

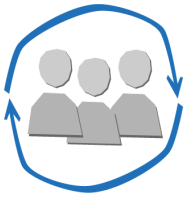
a. Date of completion

b. Length of right to work

c. Condition of working

    i. 3.4.Q3.1. Any other information not listed above. Please provide details.

Part 4: Inclusive



Introduction

The national digital ID system provides an opportunity for government to accelerate its mission towards a digitally inclusive UK, and ensure that everyone can participate in, and benefit from, a modern digital society and economy. Inclusion will therefore be at the heart of how we design and deliver this system to the public, and how we support individuals who struggle to prove their identity or engage with digital services.

Inclusion and security measures will be developed in tandem from the outset. See chapter 5.2. on security for more detail on keeping the digital ID system secure.

Chapter 4.1: Eligibility for the digital ID

All British and Irish citizens, and foreign nationals with permission to be in the UK, who are above an agreed minimum age, will be eligible for the digital ID.

Minimum age for eligibility

We plan to make the digital ID available for those who meet the above criteria and are aged 16 or older. This is because Right to Work checks are required from age 16. However, we want to gather views on either:

- lowering the minimum age of eligibility to 13, or
- removing a minimum age so that everyone can have the digital ID from birth

Such changes have advantages and disadvantages, and we invite views to inform a final decision. Regardless of the minimum age chosen, the Age Appropriate Design Code (AADC) and its principles will apply to all children using the digital ID, even 16- and 17-year-olds. Appropriate parental supervision mechanisms will also need to be designed to be proportional to the risks and benefits to the child.

Lowering the minimum age of eligibility to 13

There are currently relatively few occasions when children aged 13-15 are required to prove their age or identity. Accessing online platforms, including social media platforms,

is an important exception, as the legal age from which people in the UK can provide consent to the processing of their personal data for most online services is 13. As a result of this, many online services have a minimum age of access of 13. Additionally, the Online Safety Act 2023 requires in-scope services that do not prohibit certain types of content harmful to children, including pornography and suicide content, to use highly effective age assurance to prevent children from encountering it.

Some online services use certified DVS providers as a method of age assurance. This allows children aged 13 or over to use their services if they can sufficiently verify their identity with a DVS. However, any child that does not have access to enough evidence of their identity, like a passport, to allow online services to be confident in their age, will be unable to benefit from these services and may be prevented from accessing age-appropriate online content.

Making the digital ID available for those aged 13 and over could help address these inclusion concerns by being free for children to access and use. It could help services to accurately distinguish a child's age or age group between 13-17 and thereby deliver more tailored and age-appropriate experiences. We do not propose mandating the digital ID as the only way to prove your age or age range on online services and we will continue to support innovation and user choice in age assurance technologies.

Further, making the digital ID available to additional age groups may bring some public service benefits. Parents and guardians typically need to register and manage access to services on the child's behalf. The more complex the child's individual circumstances, the more frequently their parent or caregiver may need to provide this same information to a variety of services. Broadening access to more age bands may help to reduce this administrative burden on more parents, and support more efficient public services.

However, lowering the minimum age to 13 would also bring unique privacy, inclusion and design challenges as children's personal data must be afforded the right levels of protection. Younger teenagers are also more likely to require accessible language and inclusive parental supervision mechanisms. Additionally, explicit parental or guardian consent may be necessary for anyone under 16 to access the digital ID, or it may need to be managed entirely by a parent/guardian on a child's behalf.

Providing everyone with the ability to have a digital ID from birth

Enabling people to participate in the digital ID system from birth could support streamlined, digital, lifelong public service provision. Enabling parents and guardians to prove information about their children digitally from birth would mean that parents or guardians of younger children could have the same benefits as those of older children.

Parents or guardians would be able to decide whether to obtain a digital ID for their child. We also recognise that children under the age of 13 would not be able to manage their own digital ID. Instead, this would be done by a parent or guardian.

We further recognise that removing a minimum age for digital ID eligibility would raise additional challenges compared to having a minimum age of 13 or 16. This includes additional privacy issues, and issues around how parental management of the digital ID would work in specific instances, such as where parents are separated. We also need to understand whether children would be placed at a disadvantage if their parent or caregiver decided not to obtain a digital ID on their behalf, and if this would create new safeguarding, exclusion or other risks.

Questions about Chapter 4.1: Eligibility for the digital ID

These questions are for everyone:

4.1.Q1. All British and Irish citizens, and foreign nationals with permission to be in the UK, who are above an agreed minimum age will be eligible for the national digital ID. Are there any other groups that should be included?

a. Yes

b. No

c. Don't know

    i. 4.1.Q1.1 Please list which groups you believe should be included, and why

4.1.Q2. Which of the following ages do you think is most suitable to access the digital ID system from?

a. 16 years old

b. 13 years old

c. Birth

d. Other

e. Don't know

    i. 4.1.Q2.1. Please explain your answer

Chapter 4.2 Unlocking access across society

It is our intention that the national digital ID system enables every eligible individual to engage with the many benefits of this technology, and the resulting improvements in greater ID (identity document) ownership and increased digital inclusion. Both ID and digital exclusion are tackled in turn below.

Traditional identity document exclusion

ID exclusion is a persistent issue in the UK. In 2021, the Cabinet Office found that 1 in 10 eligible voters in England, Scotland and Wales did not hold an in-date and recognisable form of photo ID. Due to a combination of financial, practical and other barriers, many people struggle to access identity documents like passports or driving licenses, which are commonly used as proof or evidence of identity. For instance, an adult British passport is priced between £94.50 and £107, depending on the application route, which can place them out of reach for low-income individuals. In addition, some applicants for existing government IDs may struggle to obtain supporting evidence, such as birth or adoption certificates, or access to a counter signatory required to successfully navigate application processes. An individual's level of trust in government can also affect whether they choose to engage with formal identity systems in the first place.

Those without the ability to prove identity to the required standard are at a disadvantage when it comes to engaging with government and wider services, whether online or offline. In the most extreme cases, this may mean that people can struggle to open a bank account, buy or rent a home, or prove their right to work status.

The digital ID system offers a unique opportunity to support these people. It will allow them to access a free (i.e. without up-front charges for use and access) digital ID that could transform their ability to engage with relevant services and level the playing field for those currently experiencing disadvantage. It is our intention that the digital ID system enables every eligible individual to engage with modernised digital services across government. More details can be found in Part 3 on how the digital ID system will be useful.

Digital inclusion

The digital ID system will also be rolled out with a core focus on digital inclusion. Many people lack the access, skills, support and confidence to participate in and benefit from our modern digital society. Addressing this will be critical to their ability to use the digital ID. For example:

- The Lloyds Consumer Digital Index Report finds 1.6 million people in the UK are living offline, meaning they do not use the internet at all

- The Lloyds Essential Digital Skills report finds 8% of UK adults (approx. 4 million people) do not have the essential digital skills needed for everyday life
- Age UK research finds 37% of those aged over 65 who want to be online more, do not trust the internet
- Ofcom's technology tracker finds 6% of UK households do not have a smartphone

Groups requiring targeted support

Our inclusion work will focus on supporting a variety of different groups. Below is a non-exhaustive list of those who may benefit most from additional support measures to ensure they are able to access the digital ID, and a range of challenges that could limit individuals' ability to access it:

- those on a low income, who may face data or device poverty
- people who have legally migrated to the UK but struggle to prove their right to be here (people without foundational documents, like birth certificates or passports, or expired documents), such as older Commonwealth citizens and the Windrush Generation
- those with no or poor internet connectivity, or incompatible or outdated tech
- people lacking essential digital skills
- people with low motivation or confidence to use digital technologies, which may be due to lack of skills and knowledge
- those lacking support networks to access available technology
- people experiencing unemployment
- people living with physical and cognitive disabilities
- people who are neurodivergent
- older people
- children and young people, including those Not in Education, Employment or Training ('NEET'), including vulnerable young people and those in care
- care leavers
- survivors of, or those currently experiencing, domestic abuse
- people with limited English
- people who do not have a fixed or stable address, or experience homelessness
- people affected by human trafficking or modern slavery
- sex workers
- people in refuges or safe houses, witness protection, or with confidentiality or non-disclosure orders
- trans and non-binary people and anyone with recent name changes and mismatched records. This should be read alongside Part 3 which includes a section on sex and gender

- groups that facial biometric systems may not reliably recognise, for example people who live with facial differences or people who have undergone facial surgery
- people in prison, recently released or on probation
- in-patients in hospitals or secure mental health units and care homes
- cultural communities with less engagement in mainstream society, including some religious and traveller communities
- people with concerns about data use, security and data privacy, who are reluctant to engage, or do not trust digital products or government services. This chapter should be read alongside chapter 5.1 on data protection and privacy

Questions about Chapter 4.2: Unlocking access across society

These questions are for everyone:

We are committing to an inclusion programme to ensure everyone eligible in the UK can access the digital ID.

4.2.Q1. Some people may face barriers to creating or using the national digital ID. This may be due to difficulty accessing traditional proofs of identity (like passports) or due to a lack of digital access, skills or confidence.

Are you aware of any other barriers not captured in the consultation?

a. Yes
b. No
c. Don't know
    i. 4.2.Q1.1 Which other barriers are you aware of and why?

4.2.Q2. The government is committed to making sure the national digital ID system stays true to the approach outlined in the Digital Inclusion Action Plan. This includes providing local level support, increasing access to the internet and helping people develop digital skills.

Is there any particular support not captured in the consultation or the Digital Inclusion Action Plan that would help you or other people to use the national digital ID?

a. Yes
b. No
c. Don't know
    i. 4.2.Q2.1 Which other forms of support would be helpful and why?

4.2.Q3. Chapter 4.2 of the consultation includes a non-exhaustive list of those people who may benefit the most from additional support measures to ensure they are able to access the national digital ID.

Are there any groups not included in the list that you believe could also be at risk of ID or digital exclusion?

a. Yes
b. No
c. Don't know

i. 4.2.Q3.1. Please specify which other groups may be excluded and describe how they might be impacted. Please do this for each group you identify.

Chapter 4.3 Commitment to supporting inclusion

Practical onboarding support

Some individuals will require specific support to create and use the digital ID, and we will ensure that measures are in place to help them do this.

Support for onboarding and ongoing use of the digital ID could include:

- dedicated and locally accessible assistance
- support and training from trusted individuals
- guidance and programmes designed to inform and disseminate skills

An example of this is HM Passport Office, part of the Home Office, which provides additional support to those who struggle to apply for a passport. This includes commercial in-person routes in local communities to check documents and ensure the correct information is provided. Telephone support for disabled and digitally excluded customers is also provided to facilitate the correct completion of application forms. HM Passport Office also integrates safeguarding measures for vulnerable applicants, ensuring sensitive handling of personal circumstances such as disability. We will ensure that support is in place to ensure all eligible individuals can access the digital ID if they wish to.

Digital inclusion support

It will be critical that those who require digital support are able to access the digital ID system. The Digital Inclusion Action Plan sets out the steps that government is taking to improve digital skills and help more people access the benefits of technology and online services. Some examples include:

- identifying what works and designing evidence-based interventions
- taking a cross-government approach to breaking down silos
- delivering in partnership with local authorities, national and devolved governments, and private and third sectors
- learning from international partners and following best practice

Government will continue to deliver targeted digital inclusion activity to assist those who are digitally excluded, including providing support to access the digital ID.

Questions about Chapter 4.3: Commitment to supporting inclusion

This question is for members of the public:

4.3.Q1. What kind of support should be made available to people who do not have a digital device (like a smartphone or tablet) to enable them to create and access the digital ID?

a. Dedicated and locally accessible help

b. Support and training from trusted individuals

c. Guidance and programmes designed to inform and disseminate skills

d. Other. Please provide details.

This question is for experts responding in their own capacity and organisations:

4.3.Q2. We are considering dedicated accessible support for those who are digitally excluded, delivered locally, in-person and by trusted organisations. Are there any other ways you think the government should consider supporting those who are digitally excluded?

a. Yes

b. No

c. Don't know

    i. 4.3.Q2.1. Please explain what you support measures should be considered

Chapter 4.4 Accessibility

The national digital ID will follow an inclusive by design approach. This means that we will aim to:

- anticipate and remove barriers to accessibility
- design features with diverse users in mind
- extensively test features before roll-out
- ensure a good experience for all users regardless of their ability or the age or model of their device

The system will comply with recognised accessibility standards like the Web Content Accessibility Guidelines (WCAG) 2.2 AA standards. The system will also comply with the Public Sector Bodies (Websites and Mobile Applications) (No. 2)) Accessibility Regulations 2018, which set out standards specifically for public sector bodies to ensure their websites and mobile applications are accessible. It will also aim to be fully operable using common assistive technologies, including:

- screen readers
- keyboard-only navigation
- voice commands
- biometric authentication
- screen magnification

Accessibility will be an ongoing and collaborative effort, and we will adapt our approach as new opportunities for accessibility are identified and technological needs evolve.

Questions about Chapter 4.4: Accessibility

This question is for everyone:

4.4.Q1. The government intends to engage with a range of people and organisations outside of government to help ensure the design and delivery of the national digital ID system is accessible. Can you suggest any specific organisations or types of organisations which the government should engage with?

Chapter 4.5: Alternative access routes

We recognise that some groups of people may significantly benefit from alternative routes and additional support to access and use their national digital ID. The standard route, as set out in Part 2, will require a device, such as a compatible smartphone or tablet, and connectivity.

We are considering whether alternative routes to accessing the digital ID will be needed, to ensure that all eligible individuals can access the system. Any alternative route would facilitate a digitised check to ensure that the alternative route is as robust as the standard route in terms of security, reliability, accuracy and the prevention of fraud. This means that a physical card that is only visually checkable cannot be an alternative.

Below are examples of how other countries have approached an alternative but digitised access route to their respective systems. These international examples are included for reference only and the national contexts within which they have been designed are likely to vary significantly to those in the UK. They provide examples of technologies that can facilitate a digitised check without requiring a device or data connectivity.

International case studies:

- **Denmark's MitID:** MitID is predominantly accessed via the MitID app, but alternative access routes include a code display. This is a physical product which displays a one-time passcode for users to safely log in to a web browser. More information is available on the MitID website
- **India's Aadhaar:** India's digital ID system includes a smartphone app alongside alternative access routes. These alternative routes include digitally signed QR codes, which can be scanned for offline identity verification. More information is available on the Aadhaar Website
- **Estonia's E-ID:** The foundation of this scheme is a physical ID card with a smart chip for digital authentication. The e-ID system also includes a smartphone app. As an alternative access route, Mobile-ID offers secure digital authentication and signatures via a special SIM card, enabling access to e-services without a card reader. More information is available on the e-ID website

Questions about Chapter 4.5: Alternative access routes

This question is for everyone:

4.5.Q1. We are exploring alternative ways to access the national digital ID for those who cannot use a device. What do you think are the most important barriers for government to address when designing alternative access routes for the national digital ID?

This question is for members of the public:

4.5.Q2. If you are someone who does not use a digital device, what would you want from an alternative access route?

Part 5: Trusted

Introduction

It is essential to the success of the national digital ID system that government upholds the highest standards of security, privacy and data protection, with effective and proportionate governance and oversight. Individuals must have full confidence that the government is looking after their data, keeping it safe from unauthorised disclosure, fraud, cyber-attacks and other threats. Similarly, those who need to rely on information in the digital ID, from government services to private businesses, must be able to trust its accuracy and validity. Principles of data minimisation and empowering users to ensure they have greater control over how much data they share when using their digital ID at point of use will be central to the system's design and implementation.

Chapter 5.1: Data protection and privacy

The digital ID system will be designed and delivered with privacy at its core. The UK has strong data protection legislation, and robust legal requirements and principles of data protection and privacy by design will be embedded throughout every stage of development and delivery of the new system. Data protection legislation means the UK GDPR, the Data Protection Act 2018 and any regulations made under them. Other relevant legislation includes the Privacy and Electronic Communication Regulations 2003 and the Human Rights Act 1998. This legislative environment provides strong guardrails for how the digital ID system can be implemented and used, and the design and delivery will not deviate from established legal requirements.

Building on existing progress

The government already processes personal data for identity purposes, including via GOV.UK One Login, GOV.UK Wallet, the eVisa service and HM Passport Office. These services are safe, secure and designed with privacy in mind, and the new system will build on these well established and robust foundations to deliver a solution that is designed to the highest standards of privacy, security and trust.

Data protection by design is embedded into these systems and strong governance arrangements ensure that data protection compliance is integral to their operation. For instance, GOV.UK One Login only stores the minimum data required to verify someone's identity and ensures that it is being shared by the rightful holder. The GOV.UK Wallet follows a decentralised data model. This means that instead of storing everyone's personal data in a new central database, each government department or agency manages its own part of the system. They issue and maintain digital credentials (and hold the personal data necessary to do so), using their own secure infrastructure, but all these credentials can be linked and used through the GOV.UK Wallet, underpinned by GOV.UK One Login.

Building on these services, we will design the digital ID system to be secure, with only the minimum amount of data collected and stored. The majority of data used throughout the process remaining at source, where it is already securely stored. This will ensure the relationships that people already have with different government departments remain intact. For instance, data about someone's benefits entitlement will remain with the Department for Work and Pensions (DWP), even if they prove their identity to the DWP using the national digital ID.

Box 5.1.1. HM Passport Office protection of personal data

The protection of personal data is paramount to HM Passport Office and is an example of how government holds personal data safely and securely. HM Passport Office uses a multi-layered security approach, combining encrypted data stores with strict access controls for both users of the data and those maintaining the systems.

Our digital services run on modern, UK-hosted cloud infrastructure. We run the system in a securely protected, self-contained environment designed to reduce risks. Data is encrypted in transit and at rest, only authorised people can access the system, all activity is recorded, and every request is checked to ensure it's safe and legitimate.

Security is designed in from the outset. Threat-modelling is carried out as services are developed and maintained, ensuring potential risks are understood and mitigated early. This is supported by continuous monitoring and regular assurance activities to maintain the highest standards of security. HM Passport Office processes personal data in compliance with UK data protection legislation. Personal data is only kept for as long as necessary, and is not shared unless it is lawful, necessary and proportionate to do so. Full details can be found in the Privacy Information Notice on GOV.UK on how your personal data is used in HM Passport Office.

Exercising greater consent and control

While people will always have a meaningful choice about whether to use the digital ID, we are also committed to exploring design options that will support them to exercise

greater consent and control while using their digital ID. As set out in Chapter 1.2, the range of ways people can choose to use digital ID in the public and private sector will grow over time – but, crucially, people will also be able to continue using any other alternatives, like physical documents. However, for those who opt to use their digital ID, our ambition is to build in greater consent and control than physical alternatives offer.

For instance, in Chapter 3.1 we cover how the digital ID will support 'selective disclosure' functionality. Currently, when presenting or using scans of physical identity documents, individuals have no choice but to disclose all of the information printed on them. This can often include unnecessary attributes or information. By contrast, the digital ID will allow people to disclose only information about themselves that is relevant to a situation. This helps reduce privacy risks by minimising the potential for exposure of sensitive data. By allowing people to control when, where and with whom to share information from their device, this also makes someone's consent central to any interactions where they choose to present their digital ID.

We want to maximise these kinds of benefits for people. As this system develops, we will therefore continue considering how people can be empowered to exercise greater consent and control over their digital ID in other ways and in different use cases.

For clarity, references in this section to consent are not intended to be read as references to consent as defined under the UK GDPR.

Privacy by design and default

We recognise that privacy is a central concern for many individuals and organisations. We take these concerns seriously. The digital ID system will be clear about what data is collected, why it is needed and how it will be used. We welcome an open dialogue with privacy focussed individuals, organisations and communities to share their views and concerns about data protection and privacy of the system. We will work closely with stakeholders to help ensure that privacy concerns are heard and, where appropriate, addressed.

We expect that the digital ID system will offer a range of privacy benefits to users and to society, including:

- allowing people to share only the information necessary for a given transaction or to access a service (e.g. proving age over 18 without revealing a full date of birth or other information which might be seen on a physical document)
- reducing reliance on less secure means of proving identity (e.g. reduced need to share or use hardcopy identity documents and other evidence)
- ensuring greater transparency of how data is processed and who it is shared with
- simplifying businesses' privacy compliance responsibilities by introducing a simple and secure way to check an individual's right to work

While detailed arrangements for personal data processing are subject to the final design of the system and cannot be set out in detail at this time, the following safeguards will be built into the digital ID system to protect user privacy and give people full confidence in how their information will be handled:

- **Data protection by design and by default.** The system will be designed with privacy as a core principle, following "privacy by design and default" from the earliest stages. Every architectural and functional decision will prioritise user privacy, including minimising data collection, ensuring secure storage, and maintaining transparency. Privacy specialists will be embedded within the project team to review all design choices and provide guidance to ensure compliance with data protection laws. Decisions will be documented and auditable, reinforcing accountability throughout the process. As part of the UK's data protection framework, the accountability principle means that an organisation is responsible for complying with the data protection principles and must be able to demonstrate that compliance.
- **Data Protection Impact Assessments (DPIAs).** DPIAs will be central to this approach and conducted continuously throughout the system's lifecycle. These assessments will examine how personal data is processed, identify risks to individuals' rights, and outline measures to mitigate those risks. DPIAs will undergo rigorous governance, involve oversight from senior officers, and be shared with the Information Commissioner's Office (ICO) for review and advice. This ensures evolving risks are addressed promptly and compliance with data protection law is maintained.
- **Transparency and public engagement**. Transparency is central to building public trust, and we are committed to being open and accountable in how personal data is processed. The consultation process and ongoing engagement will give people a say in how the system is designed. Once these decisions are finalised, users will receive clear, plain-language information about what data is collected, how it is used, retention periods, and their rights. Privacy notices will be accessible and easy to understand, ensuring people remain informed and confident in the system.
- **Compliance with all data protection principles and requirements.** The digital ID system will comply with all applicable data protection requirements, including:
    - **Personal data will be processed fairly, lawfully, and transparently**, with clear legal bases and safeguards embedded to prevent harm or discrimination.
    - **Data will be collected only for specific, legitimate purposes**, such as verifying identity or right to work, and only the minimum necessary information will be used, regularly reviewed, and protected through technical controls.
    - **Accuracy will be maintained** via authoritative sources and user-friendly update mechanisms.

- **Data will be retained only as long as needed**, stored securely on users' devices where possible.
- **Children's data** will be handled with heightened protections, aligning with the ICO's Age Appropriate Design Code and Children and the GDPR guidance.

Questions about Chapter 5.1: Data protection and privacy

This question is for members of the public:

5.1.Q1. Are there any additional measures, beyond the principles and standards set out in the consultation, that we should consider to further protect user data?

a. Yes
b. No
c. Don't know
    i. 5.1.Q1.1. If yes, please explain which measures we should consider and why

This question is for experts responding in their own capacity and for organisations:

5.1.Q2. Principles of data minimisation and empowering users to ensure they have greater control over how much data they share when using their national digital ID at point of use will be central to the design and implementation of the digital ID system. How should the government ensure transparency around how national digital ID data is used?

Chapter 5.2: Securing the national digital ID system

Building on existing cyber security best practice and processes

The government has longstanding experience and best practice in securely protecting public systems and services that handle large personal data sets, and which are critical to day-to-day life in the UK. This includes data that proves an individual's identity. For example, HM Passport Office upholds rigorous security principles to ensure the integrity and trustworthiness of British passports, including biometric security and strict identity verification protocols. The digital ID system will build on the insights gained from existing trusted and secure models – and will need to set the benchmark for a secure, national-scale digital identity service.

It is essential that security of the systems and any data that is accessed, shared and stored is at the heart of the design. The government has identified cyber threats as a growing risk to the resilience of public services, with a sharp rise in sophisticated attacks targeting critical systems. Maintaining the highest standards of security and continuous improvement to ensure systems keep pace with evolving threats is essential to maintaining public trust and ensuring the long-term security of the national digital ID infrastructure.

All UK government digital services and technical infrastructure must comply with two core standards – Cyber Assessment Framework profiles and Secure by Design principles. The digital ID system will be underpinned by these fundamental cyber security standards, as well as continuous advice on keeping pace with the cyber threat to the UK. We will seek advice from the National Cyber Security Centre (NCSC) as the UK's national technical authority for cyber security.

Vulnerable and at-risk individuals

It is particularly important that the government takes steps to ensure that government services correctly handle the personal data of those individuals who may be vulnerable or at heightened risk of harm, such as those individuals who may experience disproportionate harm if their personal data is misused, exposed, or inadequately protected. This includes but is not limited to:

- victims of domestic abuse
- people in witness protection schemes
- government staff in sensitive roles
- high-profile public figures
- serving judges or MPs
- children or elderly individuals
- people with disabilities or mental health conditions

The digital ID system will operate in line with the government's published principles for securing personal data in relation to vulnerable and at-risk individuals. This will ensure it achieves the required balanced, inclusive approach and protects such individuals without inadvertently increasing their exposure through exclusion or inconsistent treatment of their identifying information.

National security

The government is required to ensure the digital ID system is secure and protected in the interests of national security. While detailed arrangements for security mitigations are subject to the final design of the system and cannot be set out in detail at this time, the digital ID system will be built to safeguard against national security threats.

Lawful access

Access to personal data processed as part of the digital ID system will be subject to existing legal requirements and restrictions ensuring access is both necessary and proportionate. In particular, access to personal data by law enforcement and intelligence agencies for the purpose of preventing or detecting crime, or in the interests of national security is governed by existing legislation, including the Police and Criminal Evidence Act 1984, Crime and Courts Act 2013, Investigatory Powers Act 2016 and Data Protection Act 2018. Existing powers are designed to enable the detection and prevention of serious threats, such as terrorism, espionage, and serious crime. Rigorous oversight and safeguards are in place to protect the rights and privacy of individuals.

Access to the new digital ID more broadly will also be governed by existing laws (including the UK GDPR and the Data Protection Act 2018). This is already the case for DVLA and the driving licence, HM Passport Office and the passport, and GOV.UK One Login.

Police powers

There will be no legal obligation for people to have or present the digital ID. The police will not have new powers to request an individual's digital ID for stop and search purposes.

Box 5.2.1 – Police stop and search

In the UK there is no legal requirement to carry proof of identity at all times, and this will remain the case. The police, with several limited exceptions, generally have no powers to require a person to provide them with identity documents during day-to-day encounters.

However, where immigration enforcement officers are carrying out an enforcement visit or warrant, they do have powers to ensure that all those who are employed have the right to work in the UK which may include examining identity documents.

The police have common law powers to prevent and detect crime, and must comply with various legislation such as data protection, human rights, equality and other relevant laws. For example, there is a legal basis for police use of facial recognition, which may include access to biometric data held by government. The government recognises that the current legal framework is complicated and has launched a consultation (which concluded in February 2026) on reviewing the legal framework for using facial recognition in law enforcement. That consultation proposes a new legal framework that will create consistent, durable rules and appropriate safeguards for facial recognition and similar technologies which are likely to follow it in relation to biometric data held by government in the future. The national digital ID will be subject to existing frameworks and/or to any new legal framework introduced.

Questions about Chapter 5.2: Securing the national digital ID system

This question is for everyone:

5.2.Q1. Are there any additional security safeguards to those named above that should be considered in relation to the national digital ID system?

a. Yes

b. No

c. Don’t know

    i. 5.2.Q1.1. What are they and why are you recommending them?

Chapter 5.3: Fraud as a national challenge

Fraud against individuals and businesses is a rapidly evolving and deeply harmful crime which devastates victims, erodes public trust, and poses a serious threat to the national security and economic stability of the UK. The government knows that fraud is a significant problem in both the public and private sectors in the UK, with research from the Office for National Statistics estimating fraud to be the most prevalent crime type in England and Wales. We know that fraudsters will target the digital ID system – and that ensuring we understand why, how and when will be critical to maintaining trust and keeping the system safe for use. This work will be implemented alongside the government's expanded Fraud Strategy, which was published by the Home Office on 9 March 2026.

A significant proportion of fraud in the UK is enabled by identity misuse and unauthorised account access. This occurs where criminals impersonate others, steal, buy or create false identities to access services, benefits, or financial products. In 2024, Fraudscape reported that identity fraud represented 59% of all cases filed to the Cifas National Fraud Database. Artificial intelligence (AI) has also altered the fraud landscape, introducing new and complex risks. AI can be used by malicious actors to generate highly convincing fake identities, manipulate biometric data, and automate impersonation at scale.

Tackling identity misuse is therefore critical to ensuring a secure digital identity system. The digital ID system offers opportunities to strengthen verification and authentication processes, making it harder for criminals to exploit identity-related weaknesses. Identity abuse can also occur when credentials appear dormant, outdated or the digital ID is no longer valid or required, creating opportunities for exploitation. This means it will be important to maintain identity accuracy throughout the lifecycle of the digital ID.

Box 5.3.1 - Scammers

The national digital ID will be targeted by fraudsters, scammers and misinformation campaigns. Fraudsters may impersonate government agencies, sending fake emails, scam texts or calls asking people to “register” or “verify” their digital ID. These messages could link to malicious websites designed to steal personal data or payment information. Criminals might also promote unofficial apps claiming to be the new digital ID or GOV.UK Wallet tricking users into downloading malware or submitting sensitive data. Criminals could pose as employers or government officials requesting the new digital ID’s details for right to work checks, then use that data for identity theft or fraud. Similarly, unregulated third-party services may offer to “help” users set up their digital ID, collecting personal information under false pretences.

To ensure the success and integrity of the digital ID system, we know it is essential to anticipate and mitigate the risks posed by scams and misinformation.

As outlined in Part 4, some groups may require alternative routes and additional support to access and use the digital ID. These alternative routes will be designed without compromising security and with robust fraud prevention measures built in.

Questions about Chapter 5.3: Fraud as a national challenge

These questions are for everyone:

To make sure everyone can access and use the national digital ID, the application process will need to offer alternative routes and additional support for those who need them.

5.3.Q1. We want to ensure these alternative access routes are secure. What do you think are the most important factors we need to consider in order to achieve this?

5.3.Q2. What do you think are the most important factors to consider when ensuring alternative access routes to the national digital ID are not misused by fraudulent actors?

Chapter 5.4: Ensuring strong oversight and governance

Strong governance and oversight are vital to protecting individuals' rights and establishing public trust in the national digital ID system. Robust oversight regimes often involve a combination of internal and external processes, ranging from internal complaints handling mechanisms right up to independent scrutiny and being held to account by Parliament and others.

Existing oversight structures

As set out in chapter 2.1, the government has a mature and trusted infrastructure for identifying good digital verification services, which helps ensure people's data and privacy are protected. This includes existing standards and regulatory safeguards for areas including cyber security, national security, fraud, and data protection and privacy. We intend for the digital ID system to operate within this ecosystem, adopting these standards and safeguards, to ensure the system operates to the highest standards.

There is a key role for Parliament in scrutinising the proposals for the digital ID system, its ongoing operation and, where required, any secondary legislation that is necessary. On an ongoing basis, government departments are required to annually report to Parliament on their financial performance and activities, and it is our expectation that the digital ID system will be subject to these same requirements. It is also our intention to put in place bespoke reporting arrangements that will reflect any statutory powers and duties agreed by Parliament in respect to the system. Any legislation will also be subject to post implementation review to allow Parliament to understand how it is operating.

Additional oversight arrangements

We will examine the full range of oversight options that may be applicable to the system once the final design is in place, though this work will begin with public input throughout the consultation process. Appropriate oversight will meet the needs of the digital ID system, and will:

- hold the government to account for risk management and necessary controls
- be proportionate to the burdens or restrictions imposed on the public and business
- be efficient and economical
- be suitably open and transparent, making information accessible

Of specific importance will be how people can seek resolution if they encounter issues. For example, an error with the issuance, renewal or revocation of their digital ID, or a technology failure that could lead to a negative impact on the user. It is essential that there are clear routes for individuals to make a complaint and that the process to

manage these complaints is quick and effective. The government will consider appropriate forms of redress (the process by which an issue is made right) and whether and how individuals can seek compensation, through a claim, where they may be eligible to do so.

For some existing government functions, users are provided with the ability to escalate issues to an independent party for resolution if they are not satisfied with earlier attempts to resolve their issue. We could consider a similar procedure for the digital ID system. For example, HM Passport Office has a procedure for complaints about handling passport applications that includes four steps, two of which are fully independent from HM Passport Office. Box 5.4.1 summarises the HM Passport Office complaints procedure.

Box 5.4.1: Summary of HM Passport Office complaints procedure

HM Passport Office sets out the following 4 step process for managing complaints:

Step 1: If you have a complaint about how we handled your passport application, contact our customer contact centre by phone, in writing or by using our online enquiry form.

Step 2: If you have followed step 1 and are not satisfied with our response, you can ask us to review your complaint.

Step 3: If you have followed steps 1 and 2 and are still not satisfied, you can escalate your complaint to the Independent Examiner of Complaints (IEC) within 3 months of receiving our response.

Step 4: If you are still not satisfied, you can ask your MP to request an investigation by the Parliamentary and Health Service Ombudsman (the Ombudsman). You can only do this through your MP. The Ombudsman's role is to investigate complaints by members of the public about the way government departments, and their executive agencies, have treated them.

The government will also consider support for victims of fraudulent use of their digital ID. Victims of identity theft often face significant harm, including reputational damage, exclusion from services and emotional distress. Home Office research finds victims of fraud can suffer significant emotional and health impacts, even if they have not experienced a large financial loss.

Current support mechanisms in the UK focus primarily on identity fraud, with practical advice available from organisations such as Action Fraud, Cifas, and credit reference agencies. Legal remedies and formal victim support structures for identity theft remain limited, particularly where stolen documents have not yet been used to commit a further offence. The government intends to consider how victims of digital ID misuse will be

supported, including access to credential revocation, and protection against re-victimisation. Provisions should also be made to allow individuals affected by misuse or errors to restore their digital ID quickly and securely without creating new vulnerabilities, to ensure they can access services and benefits to which they are rightly entitled. Strengthening these mechanisms builds public trust and helps ensure that the system is resilient to abuse.

Questions about Chapter 5.4: Ensuring strong oversight and governance

These questions are for experts responding in their own capacity and organisations:

5.4.Q1. What additional oversight mechanisms, if any, should be put in place for the national digital ID system?

5.4.Q2. What measures can you suggest, if any, that could be put in place to make sure people can resolve issues with their national digital ID?

These questions are for members of the public:

5.4.Q3. What additional oversight mechanisms, if any, would help you to have trust in the national digital ID system?

5.4.Q4. What measures do you think should be in place to help you feel confident in resolving any issues with your national digital ID?

Part 6: Wider Summary of Impacts

In line with all government spending, it is vital that the national digital ID system represents good value for taxpayers' money. The precise costs and benefits of the system will depend on specific design choices, so it is not yet possible to quantify or assess the full impacts of the system. The evidence gathered through this consultation and the parallel 'People's Panel on Digital ID' and technical engagement exercises, will inform a comprehensive impact assessment, which will be published alongside the introduction of legislation.

The government recognises the strong public interest in understanding the potential costs of the new system – in particular the cost to the public purse of designing and building the relevant infrastructure. Similarly, we recognise the interest in understanding the wider direct and indirect benefits that the system could unlock across the economy and our public services.

This part of the consultation outlines some initial considerations in these areas and invites views or evidence to inform further analytical and policy development. It looks at the potential impacts on households, the public sector and the economy.

Impact on households

The digital ID system will enable households to better access a range of public and private services, saving people time and effort, as well as better safeguarding their information and privacy. Identity fraud is estimated to cost households £1.8 billion per annum, and the digital ID system will help tackle this through making it harder for criminals to misuse identities that do not belong to them.

We expect the benefits to households from the introduction of a digital ID system to include the following, however this will be developed further ahead of the full impact assessment:

- **Reducing personal fraud:** The digital ID may offer security and privacy benefits, for instance via selective disclosure functionality. For example, someone purchasing alcohol would only need to verify their age, and any other personal information could be hidden, reducing opportunities for fraud. Research from Crowe shows identity fraud cost individuals £1.8 billion in 2020 and Fraudscape report this accounts for 59% of all fraud cases reported to the National Fraud Database. A small reduction in the amount of fraud would save households millions, although the effect that the digital ID system would have on identity fraud is currently unquantifiable.
- **Improving access to public services.** The digital ID system will reduce barriers to accessing public services and therefore could boost household income by

ensuring households can access the services to which they are entitled (such as Tax-Free Childcare). Analysis from UCL's Constitution Unit shows that in 2024, 15% of households with an income under £5,000 per year had no photo identification, compared to 1.6% of those with a household income greater than £60,000. Providing a free digital ID will help ensure that for all households, affordability of ID is not a barrier to accessing public services.

- **Saving time:** We expect the digital ID system to reduce the amount of time households spend proving aspects of their identity to access public services. Evidence from Canada suggests that the average Canadian spends approximately 8 hours per year either creating new or using existing ID to prove aspects of their identity; this represents an opportunity cost monetised as approximately CAD 6.1 billion (or £3.3bn) for working age adults in Canada.
- **Savings on traditional IDs:** Carrying a digital ID, rather than physical evidence, may generate savings for households by replacing lost documents. Research by the Co-Op found that the number of duplicate driving licences issued in 2024 by the DVLA was over a million. The cost of a replacement driving licence is £20, so there is a potential saving of up to £20 million annually if the new digital ID leads to a reduction in applications for replacement driving licences. However, some of this benefit will already be captured by the introduction of digital driving licences, and households may still require replacement physical documents in certain use cases.

We expect there to be no direct costs to households from the introduction of the digital ID system, as households will not be charged any fees to create, access or use their digital ID. However, there is potential for households to experience the following indirect costs:

- **Familiarisation cost:** Households will need to devote some initial time into setting up the digital ID and familiarising themselves with its functionality. For the 8% of UK adults (approx. 4 million people) who do not have the essential digital skills needed for everyday life, this may involve a greater time cost.
- **Finding a suitable device:** In order to use the digital ID via the standard route, households would need to have a compatible device, such as a smartphone or tablet. For the 6% of individuals without a compatible device, purchasing one would represent a cost. However, as part of the system, we will launch an inclusion programme to ensure those who do not have a compatible device are not excluded, and there is no legal obligation for people to have or present the digital ID, so this cost can be avoided.

Impact on the public sector

The introduction of the digital ID system aims to streamline digital public service provision, as well as save taxpayers' money and lower costs to government by reducing reliance on paper-based identity documents which can be more easily faked. DWP estimates that there is £10bn of benefit fraud and error every year, and a good digital ID solution (with high quality data systems embedded in it) may be able to make a significant dent in that problem.

We expect the benefits to the public sector from the introduction of the digital ID system to include the following, however this will be developed further ahead of the full impact assessment:

- **Modernising public service delivery:** If we develop a universal unique identifier (or similar approach) tied to the digital ID and GOV.UK One Login, this would generate efficiency savings by allowing government departments to match individuals across services. Currently, it is difficult for government departments to know when it is the same person accessing different services as they use multiple identifiers, such as passport and National Insurance numbers. The digital ID will also ensure that multiple government bodies would not need to carry out the same identity checks; GOV.UK One Login has already reduced duplication in accessing public services online, and the national digital ID could enable further reduction in duplication for in-person access to public services. This could reduce bureaucracy and support departments in delivering the £14bn of efficiency gains by 2028-29 as set out in the Government Efficiency Framework.
- **Making it harder for fraudsters to falsely claim government benefits:** Further work is needed to identify the impact of introducing the digital ID system on benefit fraud, but cases of malicious use of IDs to access benefits do occur. In 2024, five members of an organised criminal gang were convicted of falsely claiming £54m using thousands of fraudulent Universal Credit claims, supported by stolen identities and faked documents. The digital ID will allow government to more easily verify an individual's eligibility for benefits and may help tackle organised crime cases such as these. However, as uptake of the digital ID is voluntary, there is still scope for malicious actors to exploit vulnerabilities in the system with traditional identification methods.

At this stage of development, it is not possible to definitively estimate the cost to government from developing and running the digital ID system. Key aspects of the policy design are subject to this consultation, and final decisions on those matters will materially impact the costs involved in setting up the digital ID system.

We expect costs to government from the digital ID system to cover the following broad areas:

- **Development costs to design, build and issue the digital ID**: This includes the core necessary expansion of HM Passport Office, GOV.UK One Login and the GOV.UK Wallet.
- **Operational costs to support scaling up**: This includes expanding support functions such as fraud prevention, security operations and user assistance.
- **Support for ID and digitally excluded users**: New operational costs to support the inclusion of individuals who do not currently hold traditional identity documents (like a passport) or are digitally excluded. This will require changes to government systems and a potential increase in dedicated caseworker capacity, such as extended face-to-face and assisted digital support channels.
- **Checking credentials**: The government will develop a credential checking service for use within government, and potentially the wider economy (per Chapter 2.2).
- **Adoption**: To support wider adoption across government, support will be available to departments and local authorities to integrate the digital ID system into their services. A national communications campaign will be launched to raise awareness of the system and encourage adoption. This will help people and businesses understand the benefits of using a digital identity, including the digital ID, and how to access their credentials.

Impact on the Economy

The Data (Use and Access) Act 2025 impact assessment estimated that the increased use of private sector digital identities will deliver £4.3 billion of net economic benefits to the UK over the next 10 years (this figure includes benefits to individuals as well as organisations). Should the digital ID increase the rate of adoption of these services, the actual economic benefits would be higher. Aside from the impacts detailed above, we expect that the digital ID system will primarily impact four key segments of the economy in the UK:

- The existing Digital Verification Services (DVS) sector
- Relying parties
- Employers
- Illegal Workers

Impacts on the existing DVS sector

The digital ID system aims to accelerate societal uptake of digital identities beyond previous expectations. This could benefit the private DVS sector by making individuals

and businesses more familiar with digital verification and cognisant of its benefits. In this case, the absolute value of the private provider share of the market may increase, even if some of the market is taken up by the government service.

Additionally, as outlined in Chapter 2.1, it is intended that the existing market of trusted DVS providers will play an important role in sharing information from the digital ID into the wider economy. This could be through performing the role of orchestration services, holder services or as identity services which derive information from the new digital ID and offer 'value add' services. This could lead to further growth and employment opportunities in the private DVS sector, which in 2023/24 generated an estimated £2.1 billion annual revenue, with £888 million Gross Value Added (GVA) and 10,246 full-time equivalent (FTE) employees.

Conversely, there may be some negative impacts on private sector providers, depending on how the national digital ID system operates. There is a risk of market displacement if the national digital ID functions as a close substitute for services currently supplied by private DVS providers, leading to negative labour market impacts. The scale of this displacement will depend on several factors, including:

- **Functionality of the digital ID:** the digital identity market is comprised of firms offering a variety of different (heterogenous) services. The extent of any impact will vary depending on the functionality built into the national digital ID and the degree to which it can provide the same services currently offered in the private sector
- **Availability of the Government Checker service:** the Government Checker may be available beyond the public sector in a limited or full capacity, or not at all (outlined in Chapter 2.2). Increased availability of the Government Checker increases the risk of displacement for private providers
- **Pricing model of the Government Checker service:** the relative cost of using a private sector service as compared to the Government Checker will influence the extent to which the government provision displaces private offerings. Displacement is more likely if the Government Checker is free at the point of use

It is important to note that individual firms may experience changes in the DVS market differently, depending on their characteristics (e.g. firm size).

Finally, investment uncertainty may have a negative impact on the UK digital identity sector. While the sector has, to date, demonstrated strong investment appeal, members of the digital identity ecosystem believe uncertainty around government policy is negatively influencing the growth of the sector. Until the design process is complete and communicated effectively, investors and organisations may delay planned investments into the sector until they can be confident the digital ID system will not reduce the value of the investment. Others may cancel their investment plans or invest in other sectors instead.

Impacts on relying parties

We expect relying parties across the economy to benefit from greater opportunities for digital verification. Digital solutions can offer faster and more secure processes, whether conducting simple age verification checks, onboarding new staff, or meeting regulatory requirements with Know Your Customer checks. It can be complex to disaggregate the benefits that the new digital ID system will bring to relying parties from those which will come from digital verification more broadly. For instance, the impact assessment for the Data (Use and Access) Act 2025 already estimates that uptake of digital identities in the UK economy will increase in the coming years. However, the national digital ID system will aim to go further by lowering costs and expanding coverage, particularly among people who are currently ID excluded.

On the other hand, organisations may incur new one-off and ongoing costs associated with the system. Examples of one-off costs include familiarisation and transition costs to understand and meet new legal requirements and business needs. For example, employers may conduct a legal review to evaluate the legislation that enables the system and its implications for their organisation. Examples of possible new ongoing costs are additional operating costs, additional audit processes or licensing fees. For instance, a company may procure new technology services in order to securely take information from digital IDs. However, some of these additional costs may be offset by reductions in costs associated with manual checks and the record keeping burden.

Impacts on employers

We expect that employers will benefit from the introduction of the digital ID through easier compliance with the existing right to work scheme. Since 2008, employers have been required to carry out prescribed right to work checks prior to employing someone in order to invoke a statutory excuse against liability for a civil penalty, in cases where illegal working is later discovered (the right to work scheme).

A representative survey of UK businesses exploring employers' understanding and implementation of right to work checks found that 89% of employers understand basic requirements. However, knowledge gaps persist and can lead to errors: small firms, those hiring agency or zero-hours staff, and construction companies are most at risk. Common mistakes include accepting invalid documents, poor record-keeping and missing follow-up checks for temporary visa holders.

In terms of recruitment, most businesses conduct checks before a contract is signed or before someone starts work, however some (39%) did so before an interview. Most employers said that employees found it easy to supply the right documents, but 11% said employees find it difficult.

Most businesses conducted manual checks (79%), but some had experience of digital provider checks (23%) and/or digital immigration checks (37%). Those that conducted

manual checks were asked further details, with most confirming that they checked original documents (92%), made copies of the documents (87%) or carried out follow-up checks if the employee's right to work is time limited (85%).

Factors such as recruitment frequency, internal processes (e.g. whether checks occur before or after interviews), and the individual circumstances of the prospective employees influence both the duration and ease of recruitment. These variables will also influence any digital system and its potential savings benefit. Cost analysis in the *Extension of Prohibition on Employment to Other Working Arrangements Impact Assessment* assumes checks using Identification Document Validation Technology (UK nationals) take 1 minute while immigration online checks are closer to the time of a manual check (5.5 minutes plus).

Impact on illegal workers

Through making it easier for employers to comply with right to work checks, the digital ID system may increase the number of right to work checks carried out in the UK and thereby aims to reduce illegal working. HMRC research identified that 'ghosts', who reported that they have not declared any of their sources of income (whether taxable or non-taxable) to HMRC, contributed £0.6 billion to the tax gap in 2023/24 (however, we do not know what proportion of these have a legal right to work in the UK).

Home Office research has found that many businesses acknowledged that illegal working was common in their sectors (21%), rising to around half of businesses in construction, food and accommodation, with employers highlighting various drivers for this. Research found that employers could be at risk of accepting the wrong documents, as 62% of employers wrongly stated that driving licences could be accepted to prove someone's right work in the UK. Furthermore, there is evidence indicating that the absence of checks, such as for self-employed workers, can generate risks of illegal working.

A streamlined approach to checks will likely improve compliance, particularly where businesses have not complied correctly with checks or where employers are deceived through false documentation, thereby reducing fraud.

The Home Office has an ongoing programme monitoring access to work, benefits and services; this includes the implementation of right to work.

Questions about Part 6: Wider Summary of Impacts

These questions are for everyone:

6.1.Q1. Do you think there are any other benefits for businesses from introducing the national digital ID system that have not been considered?

a. Yes

b. No

c. Don't know

    i. 6.1.Q1.1 If yes, what do you think these benefits would be?

6.1.Q2. Do you think there are any other costs to businesses from introducing the national digital ID system that have not been considered?

a. Yes

b. No

c. Don't know

    i. 6.1.Q2.1 If yes, what do you think these costs would be?

6.1.Q3. Do you think there are any other benefits for households from introducing the national digital ID system that have not been considered?

a. Yes

b. No

c. Don't know

    i. 6.1.Q3.1 If yes, what do you think these benefits would be?

6.1.Q4. Do you think there are any other costs to households from introducing the national digital ID system that have not been considered?

a. Yes

b. No

c. Don't know

    i. 6.1.Q4.1. If yes, what do you think these costs would be?

6.1.Q5. Do you believe there are any other wider impacts from introducing the national digital ID system that have not been considered in this consultation?

a. Yes

b. No

c. Don't know

i. 6.1.Q5.1. If yes, what do you think these wider impacts would be?

E03528850
978-1-5286-6190-4