SEPTEMBER 2025

ALEXANDER IOSAD
LAURA BRITTON
TIM RHYDDERCH
ALAN WAGER

Time for Digital ID: A New Consensus for a State That Works

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Contents

Contributors: Jo Puddick, Ryan Wain

Executive Summary

It is time for digital ID. The British public is running out of patience with a state that does not work, where interactions with public services are beset by inconveniences and delays even as outcomes slip and costs rise.

Citizens are rightly expecting the government to deliver common-sense solutions or make way. Digital ID is one such solution – and there is a massive political upside for those who embrace it. Build a system that works and voters will respond.

A modern digital ID does three things. It allows people to prove that they are who they say they are, prove that certain things about them are true, and seamlessly and securely access services on that basis. Far from reflecting the "papers, please" caricature of an ID card, digital ID is the foundation of a new system that brings fairness, control and convenience to people's everyday interactions with each other and with the state.

In a media landscape dominated by outdated narratives and unfounded fears, it may be easy to assume that no matter the benefits, the public will reject the idea of digital ID altogether. Nothing could be further from the truth.

Public-opinion research commissioned by the Tony Blair Institute for Global Change (TBI), published for the first time in this paper, shows that digital ID enjoys majority support among the British public, with 62 per cent in favour and just 19 per cent opposed.

This support is not party-political. Those who intend to vote Labour or Conservative are equally likely to favour the introduction of a digital ID. Potential Reform UK voters, despite the party leadership's opposition to the idea, are twice as likely to support digital ID than they are to oppose it.

When respondents are segmented based on their outlook on life, views on technology or key concerns, most think digital ID is an idea whose time has come, with groups representing 75 per cent of respondents showing a net positive attitude.

Frustrated by the status quo, respondents in these groupings see a role for technology in addressing the big challenges faced by the state and the everyday problems they encounter interacting with it. They want to see government do more.

Digital ID should not be seen as either a silver bullet or a minor improvement to existing systems. Instead, it should be understood as a necessary piece of infrastructure that makes it possible for government to drive radical, effective reform across a wide range of policy issues.

Digital ID can help close loopholes that trafficking gangs and unscrupulous employers currently exploit, reducing pull factors driving illegal migration to Britain and restoring control over borders. It can radically speed up citizens' interactions with government, cutting bureaucracy and reducing errors and opportunities for identity fraud.

Most importantly, it can underpin a new model of public-service delivery by acting as the front door to all kinds of everyday tasks – from viewing records and tracking applications to reporting potholes or receiving reminders to vote. A digital ID "superapp" should become the government's flagship project – a symbol of tangible change and the Reimagined State in action.

Digital-ID systems are more secure, private and efficient than mechanisms in place today. They put citizens in control of their data, bolstering transparency and making unauthorised access or significant privacy breaches like the Afghan data leak far less likely. They minimise the amount of unnecessary information that people might have to share during everyday interactions – such as proving their age to buy a pint at a pub. They allow each citizen to obtain the services they need, when they need them.

To build such a system, a shift in mindset is needed. Digital ID cannot go the way of the HS2 rail project, plagued by delays and cost overruns. To make digital ID a success, government should:

- Make digital ID a flagship programme – an exemplar for building digital tools for citizens and a top priority both for the Department for Science, Innovation & Technology and the Prime Minister's Office.
- Assemble a crack team of technologists, policymakers and user researchers, working under the direct supervision of a dedicated Digital-ID Delivery Unit backed by the prime minister's authority.
- Accelerate the integration of the existing One Login system in government departments and roll out first use cases for right-to-rent and right-to-work checks, swiftly followed by other central- and local-government tasks.
- Ensure the system becomes the universal method for verifying identity, by issuing a verified One Login to every resident over the age of 18, with fallback systems – such as physical QR codes or kiosks to access the digital-ID system in the cloud – for those who do not want or cannot use smartphones.
- Adopt an iterative approach from the beginning that incorporates user feedback quickly and releases funding as milestones are achieved.

Previous TBI research has shown that people prize delivery over ideology and want to see parties that drive genuine change. This kind of disruptive-delivery agenda can find broad support across the political spectrum. Done right, digital ID can be a foundational building block of disruptive delivery – and the strongest possible signal from the government to the British public that it is able to rebuild a state that works.

01

What Is Digital ID?

Society is built on trust. Fundamental to that trust is the ability of each individual to establish who they are and, in turn, know who they are dealing with. In every society, there are situations in which people need to prove things about themselves – name, age, address, for example. Around the world, the emergence of digital-ID systems means this has become a solved problem – and yet the UK remains a stubborn outlier.

In a media environment dominated by decades-old debates about ID cards and fictional "papers, please" scenarios, it has been too easy to lose sight of what a modern digital ID can do, its functions and the ways in which technology allows for safe, secure, private systems that go beyond identity verification to transform the relationship between citizens and the state.

The time has come for a digital ID that would bring fairness, control and convenience to people's everyday interactions with each other and with the state.

In simplest terms, a digital ID allows people to:

- **Prove that they are who they say they are.** Digital ID is a verifiable document with basic information about a person, such as their name and photo – much like a passport or driving licence. Unlike a physical document, a digital ID is never out of date, can always be to hand (for example, on a smartphone) and can't be lost or physically stolen.
- **Prove that certain things about them are true.** Linking verified information about an individual, often held in different places, to a single digital ID makes it easy to prove their age, address, migration or employment status, and more. Forms and reams of paper bills become obsolete. Citizens can choose to share only the most relevant information (for example, that they are over 18 or their confirmed address), making the system more private than traditional methods of verifying these details (which would disclose, for example, their full date of birth or size of their energy bill).

- **Access services based on who they are and their circumstances.** By cross-referencing information held by different departments, government can proactively identify and offer services to those who need them, when they need them. For example, child benefit can be offered automatically based on NHS records of a birth and HMRC data on earnings, without the need for recipients to fill in forms or disclose additional information. A new kind of personalised, always-on, data-driven public services becomes possible.

A digital-ID system typically includes an app or web interface that citizens can access at any time, with an accessible fallback (a card, printable QR code that others can scan, or kiosk) for the small proportion of the population who cannot or do not want to use them. Biometrics, similar to Apple's Face ID and other smartphone security systems or those used by banks to safeguard accounts, ensure only the ID's holder has access to their account. This replaces the current onerous and insecure ways of proving identity, such as gathering three months of bills. The digital ID acts as a verifiable "source of truth", closing off loopholes that unscrupulous employers or landlords exploit today and making identity fraud all but impossible.

In the background, a digital ID should link information held by different government bodies about the same person without moving the data or creating a single large database, instead operating as what is known as a federated system. Through the digital-ID interface, citizens should be able to see and share information about themselves, choosing the right level of disclosure in each case. They should be able to see what information the government holds about them, why it was collected and how it is being used, so that they can correct any mistakes or raise an alarm if it is used inappropriately. Audit trails mean government employees who overstepped boundaries could be identified and dismissed.

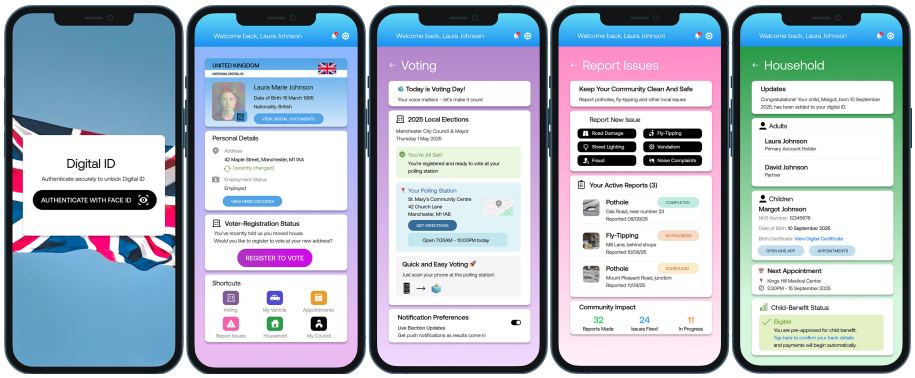
Most importantly, a digital ID should become each citizen's personal digital public assistant – a front door to the delivery of a new model of public services that are personalised, easy to access and efficient. From reporting potholes and hearing back when they have been fixed to receiving

personalised health-prevention advice or finding a child's school report in seconds; from tracking the progress of applications in real time to receiving skills-based recommendations on which jobs to apply for – a digital ID can be a citizen's command centre, placing them firmly in control of their relationship with government and ensuring they feel the impact of effective delivery in their everyday lives.

Digital ID is a generational opportunity to transform how citizens deal with the state and how the state serves citizens.

FIGURE 1

How digital ID might work



Note: The images are provided for purely illustrative purposes to showcase what the proposed system with integrated AI capabilities, based on technology available today, could look like. The illustrations and text within them should not be taken to represent a production-grade IT system.

02

Digital ID Enjoys Broad Public Support in the UK

Though long within technical reach, the transformational opportunity of digital ID in the UK has been held back by political hesitation. At a time when the country is crying out for a state that delivers, that hesitation can no longer be justified.

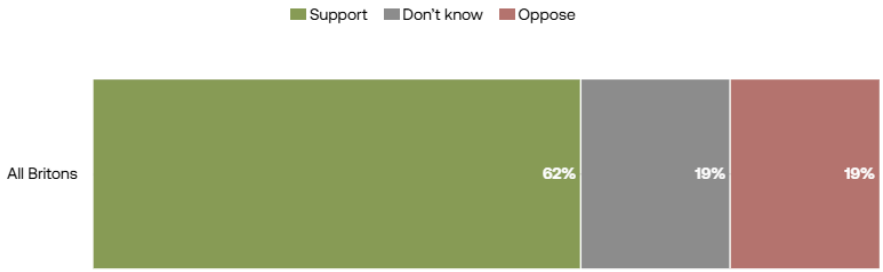
The success of this reform will depend on whether citizens accept it. From public discourse and media discussion within the UK, it might appear that support for digital ID is lacking. To test this assumption and explore the public debate more rigorously, TBI commissioned market-research organisation Yonder in June 2025 to explore public attitudes to the introduction of digital ID and, more broadly, the use of technology across public services. Results were weighted to reflect the UK population in terms of gender, age, region and social grade.

Contrary to prevailing perceptions, the survey found strong, majority public support across Britain for the introduction of a digital-ID system. After the data-sharing implications and public-policy applications of digital ID are presented, 62 per cent support the idea, compared with just 19 per cent who oppose it.

This net support of +43 per cent in favour of its introduction broadly mirrors the majority support found by the research organisation More in Common in late 2024 and the majority support which Ipsos most recently captured in favour of national identity cards.[1,2]

FIGURE 2

Overall, support for the principle of digital ID outweighs opposition by three to one



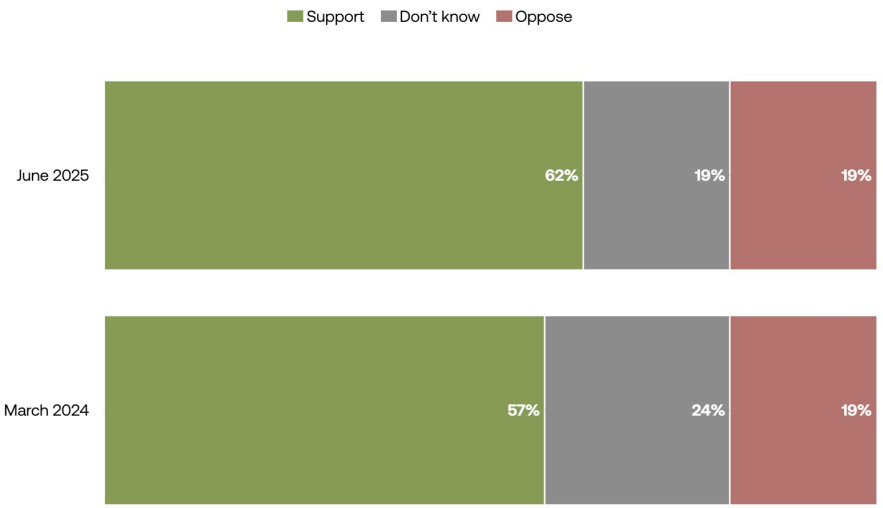
Q: Having thought more about it, to what extent would you now support or oppose the UK introducing a digital-ID system?

Source: Yonder for TBI

Our data also show that UK public sentiment continues to move towards the introduction of digital ID. When TBI and Yonder asked the British public the same question in March 2024, 57 per cent supported and 19 per cent opposed the introduction of the system – a shift in support from net +38 per cent to +43 per cent.

FIGURE 3

Support for digital ID slightly increased between 2024 and 2025



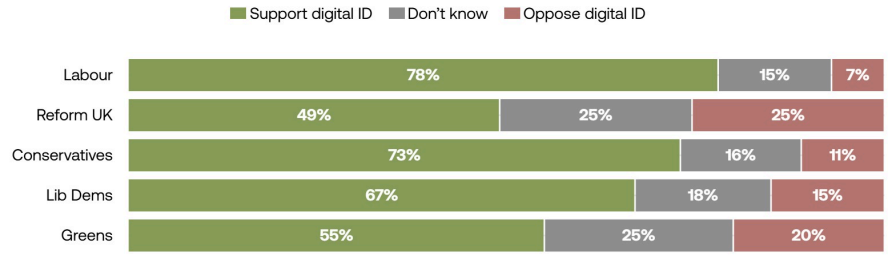
Q: Having thought more about it, to what extent would you now support or oppose the UK introducing a digital-ID system?

Source: Yonder for TBI

When broken down by current voting intention, support for digital ID outweighs opposition by two to one or more across all parties.

FIGURE 4

Support for digital ID is seen across all major parties



Q: Having thought more about it, to what extent would you now support or oppose the UK introducing a digital-ID system?

Source: Yonder for TBI

Note: Due to rounding of the polling data, the data visualisations may not add up to exactly 100 per cent.

If it were ever true that the British public was uniquely opposed to the introduction of digital ID, it is certainly not the case today.

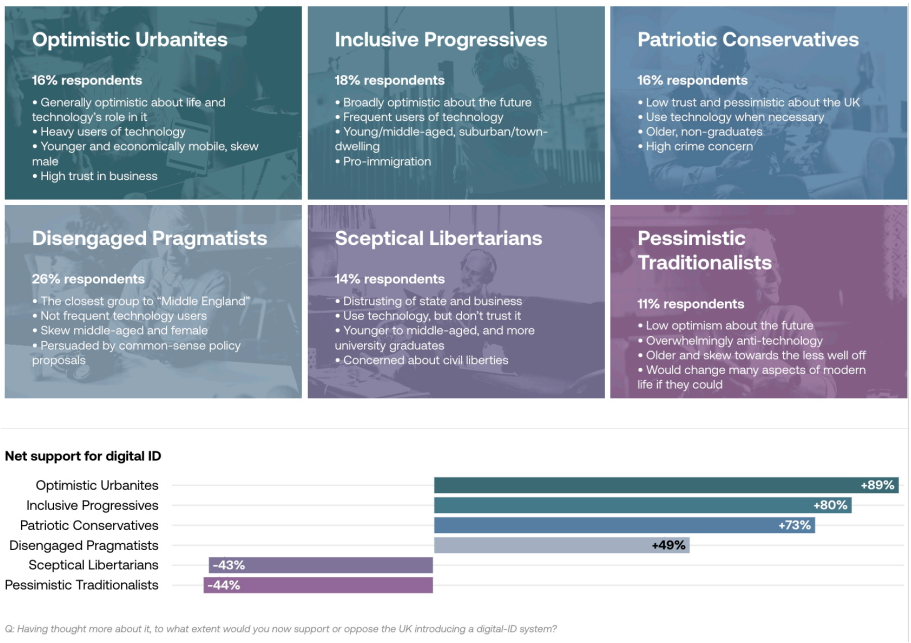
This overall support for a digital-ID system is important. But obtaining a granular understanding of who supports and who opposes the principle of a digital-ID system, and why, is equally crucial to understand its political viability.

To explore this, Yonder and TBI conducted a segmentation analysis of the British public. We asked questions that tapped into respondents' underlying political and social attitudes, their optimism about the future, stances on civil liberties and technology, and attitudes to public services. This segmentation highlights not just who supports or opposes digital ID, but what drives them – and how their broader worldview shapes their openness to different uses of the system across public services.

This tells us how the implementation of the system can assuage the concerns of the minority opposed to it and meet the varying demands of different groups across the supportive segments.

FIGURE 5

Mapping support for digital ID across six segments of social and political attitudes



Source: Yonder for TBI

Note: Due to rounding of the polling data, the data visualisations may not add up to exactly 100 per cent.

Four out of six of these groups that emerged from this segmentation start with strong net support for the principle of digital ID.

Optimistic Urbanites (16 per cent of the sample) are enthusiastic adopters and heavy users of technology. They are young, economically mobile and skew male with high levels of institutional trust.

Inclusive Progressives (18 per cent) are broadly socially liberal and optimistic about the future. They are pro-immigration and pro-public-sector investment, and generally younger to middle-aged, living in suburban areas and towns.

Patriotic Conservatives (16 per cent) are relatively distrusting and pessimistic, but open to government use of data in the right circumstances. For this group, issues of order (controlling crime, immigration and benefit fraud) resonate. They are older, tend not to have gone to university and skew towards the north of England.

Disengaged Pragmatists (26 per cent of the sample) are the largest segment – and arguably the most reflective of "Middle Britain". They are neither strongly opinionated or ideological, and they tend not to be frequent users of technology. While they are wary of unnecessary hassle or risk, they can be persuaded by policies that resonate as common sense and practical.

Opposition is concentrated among two groups.

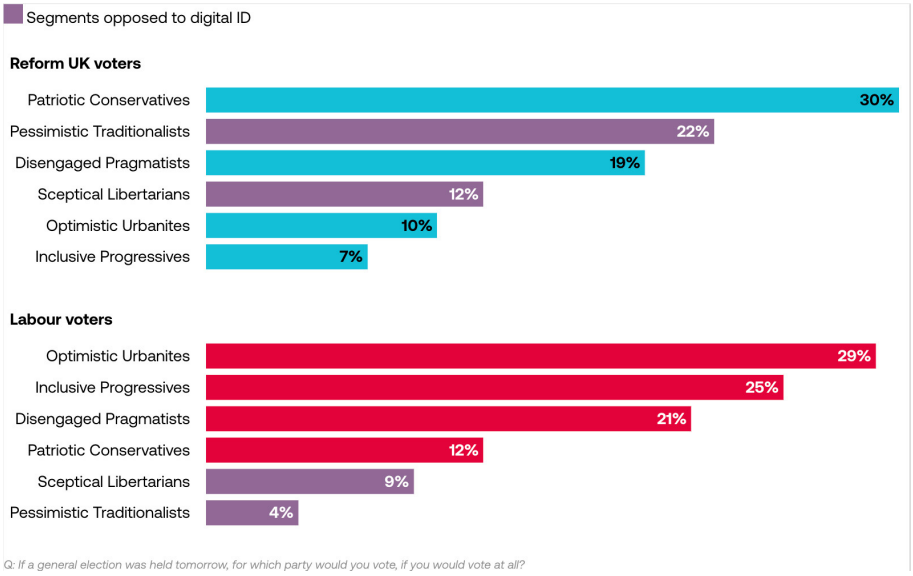
Sceptical Libertarians (14 per cent) are largely preoccupied with civil-liberties arguments. They are distrusting of state and business, skew younger to middle-aged and are more likely than average to have attended university.

Pessimistic Traditionalists (11 per cent) are overwhelmingly worried about the increasing use of technology across society. They are worried about the pace of change more broadly and would change many aspects of modern life if they could. They are predominantly older, less well off and living outside urban environments.

The six segments do not by themselves capture the political allegiances of their members, but rather their underlying world views. The political upside or risk of embracing digital ID will, in turn, depend on whether a strong enough coalition of potential voters would support its introduction. To better understand the likely shape of such a coalition, we mapped the segments to the respondents' voting intention. The difference in how Labour and Reform UK supporters are distributed across these segments highlights the political dynamics that will influence its viability.

FIGURE 6

How current Reform UK and Labour voters map onto our digital-ID segments



Source: Yonder for TBI

Over 70 per cent of Reform UK supporters are concentrated in three groups, two of which are supportive of digital ID. The largest share sit within the Patriotic Conservatives group, who are strongly supportive. These are Reform supporters who live disproportionately in key Labour-held seats in the north of England. A smaller but still significant share are Pessimistic Traditionalists – the group with the lowest levels of trust and most socially conservative views.

This research suggests that the issue of digital ID is divisive among Reform UK's potential voters, with a larger group supportive of digital ID, underpinned by its wide-ranging benefits for communities and law and order, and a smaller core group who are opposed to it, driven by complete distrust in the system and civil-liberties arguments. This split has already begun to play out in internal party debates.[3]

By contrast, current Labour support is concentrated in the four segments with strong baseline support for digital ID. The two groups most favourable to its introduction are also the top segments among Labour supporters, meaning Labour supporters are, in effect, united on this policy.

For each of the other parties, the picture is different – though with segments supportive of digital ID dominant. Over three-quarters of current Conservative supporters are spread across three supportive groupings, Patriotic Conservatives, Disengaged Pragmatists and Optimistic Urbanites. A majority of Liberal Democrats fall into either the Inclusive Progressives or Disengaged Pragmatists. Green Party support is concentrated in Inclusive Progressives, though it has the highest percentage of Sceptical Libertarians of all parties.

These patterns demonstrate that sceptics of digital ID are a minority across all parties. The potential for a broad cross-society appeal around digital ID to help solve a range of public-policy issues is significant. The political risk of digital ID therefore comes down to delivery rather than acceptance, whereas the potential upside of a system that achieves its goals is remarkable.

It is within this context that our paper *Disruptive Delivery: Meeting the Unmet Demand in Politics* set out a clear message to progressive and mainstream parties: disrupt or be disrupted. At the heart of this agenda is a commitment to transformative, system-wide change through innovation and new technologies. The introduction of a universal digital ID should form a central pillar of such an approach: bold, practical reform that delivers fairness, control and convenience, helping to rebuild trust in political institutions.

03

Digital ID Can Deliver Fairness, Control and Convenience

For digital ID to fully meet its transformative potential, it should be treated not as a silver bullet for any one political problem, nor as a marginal improvement to existing processes such as age verification. Instead, the government should commit to a vision of a universal, fully-integrated, citizen-centric digital-ID system that serves as the front door to a new generation of public services, empowering citizens to exercise control over their data and interactions with the state, and helping significantly reduce fraud and other forms of serious and organised crime. Its impact would be felt across a wide range of policy areas, from immigration to health and welfare, offering a tangible demonstration of delivery rather than delay.

Reducing Drivers of Small-Boat Trafficking and Improving Enforcement

Most recently, the debate over digital ID has been dominated by its potential to help reduce illegal migration inflows and address public concerns that the government has lost control of Britain's borders.

The UK remains one of the only European countries without a digital-ID system, a gap that makes it easier to live and work illegally. Criminal networks have exploited this weakness by selling fake passports for around £12,500.[4] These documents can allow holders to avoid eGate biometric checks in favour of older manual verification processes, where scrutiny is less consistent.

The implications of this gap can be seen in the size of the UK's shadow economy: in 2023, the value was estimated at £179 billion, over 5 per cent of total gross domestic product.[5] Although no official figure exists for the number of people currently in the UK without leave to remain, the most recent estimates range from 600,000 to 900,000.[6]

Over the past decade, the UK has steadily tightened immigration enforcement, with the aim of deterring unlawful migration by restricting access to essential services for those without lawful status. Since 2014, legislation has mandated immigration-status checks by employers, landlords and banks, with significant penalties introduced, including a tripling of fines for hiring illegal workers in 2024.

Despite these efforts, immigration enforcement in the UK remains fragmented, reactive and prone to error. Checks for the right to work, rent or access financial services are still largely manual, often misunderstood and, critically, easy to circumvent. Right-to-work and right-to-rent checks are still largely paper-based, with compliance undermined by widespread misunderstandings: more than 60 per cent of employers, for example, wrongly believe that recruitment agencies, rather than the employers themselves, are responsible for conducting right-to-work checks.[7]

Enforcement activity has intensified in the past year. According to data from the Home Office, there were 7,130 illegal-working arrests in the period from July 2024 to June 2025, up 51 per cent from 4,734 arrests between July 2023 and June 2024.[8] Since July 2024, 1,508 civil penalty notices have also been issued, with employers facing fines of up to £60,000 per illegal worker.[9] Yet ambiguity in the rules setting out how employers and landlords fulfil their legal obligations fuels non-compliance and multiplies grey areas. These shortcomings are most frequently exploited in high-churn sectors such as construction, hospitality and informal rental markets, where the combination of ambiguous requirements and limited oversight creates a porous system in which illegal work and unlawful residence persist despite clear legal prohibitions.

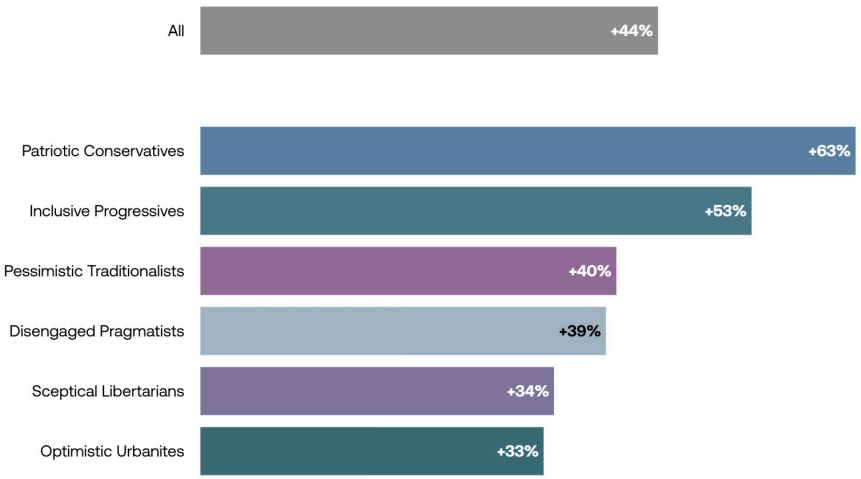
A secure, government-issued digital ID could address these structural weaknesses. Digital ID does not directly target rogue employers or criminal markets, but it does reduce the scope for them to operate by disrupting the enabling factors of the shadow economy – the loopholes that allow them to circumvent rules around the entitlement to rent, work and carry out financial transactions. This removes a key selling point for international trafficking gangs, who market the UK as an easy place to evade detection.[10]

By mandating that service providers verify immigration status through a secure platform such as the GOV.UK Wallet, status checks would become seamless, consistent and automatically logged.[11] Each verification could be recorded in a compliance ledger, enabling real-time oversight, audit and early detection of irregularities. This would replace ad-hoc enforcement with systemic deterrence. Automated alerts could also notify individuals and service providers ahead of visa expiry, reducing inadvertent overstays and making renewals a proactive process.

Our polling demonstrated that the public sees the increased use of digital technology as a plausible part of the solution on migration. Across our digital-ID segments, we found strong support for the idea that technology could be utilised by the government to greater effect to manage the UK's borders. The two segments most supportive are Patriotic Conservatives – the group where Reform over-indexes – and Inclusive Progressives – the group in which Liberal Democrat voters are most likely to sit.

FIGURE 7

All digital-ID segments support more effective use of technology to manage UK borders



Q: Thinking about the following policy challenges facing the government: Do you think there is digital technology that could help tackle these issues but is not being fully used by the government at the moment – or do you think the government is already using digital technology to appropriate effect in these areas? Technology could be used more effectively to tackle this issue. Policy challenge: Processing asylum seekers and managing the UK's borders.

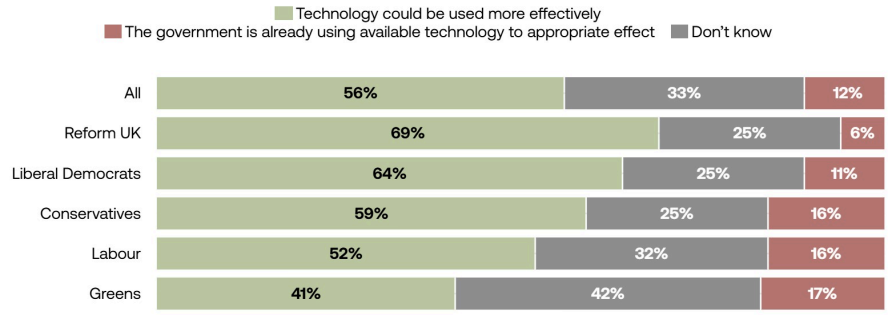
Source: Yonder for TBI

Note: Net support calculated as per cent support minus per cent oppose, excluding don't knows and non-responses.

This is reflected when we use the lens of current voting intention: there is majority agreement across voters for all parties that technology could help with processing asylum seekers and managing the UK's borders, apart from Green voters, who express greater uncertainty. But it is voters for Reform and the Liberal Democrats who are most likely to agree with the idea that greater utilisation of digital technology provides a possible route to better managing the challenge of illegal migration.

FIGURE 8

Reform UK and Liberal Democrat voters are most likely to say that technology could be better utilised to manage the UK's borders



Q: Thinking about the following policy challenges facing the government: Do you think there is digital technology that could help tackle these issues but is not being fully used by the government at the moment – or do you think the government is already using digital technology to appropriate effect in these areas? Policy challenge: Processing asylum seekers and managing the UK's borders.

Source: Yonder for TBI

In this sense, a digital ID offers a rare opportunity to unite voters across the political spectrum around delivery on migration – shifting the debate towards tangible, workable solutions that reduce the "pull" factors.

A well-designed, modern digital-ID system can disrupt the drivers of illegal migration, making it harder to work or reside in the UK unlawfully. But it should not be seen as a tool limited to tackling small-boat crossings. Digital ID can serve as the foundation for transforming public services, enabling a shift towards streamlined, citizen-centred delivery across the state.

Streamlining Interactions Between Citizens and the State

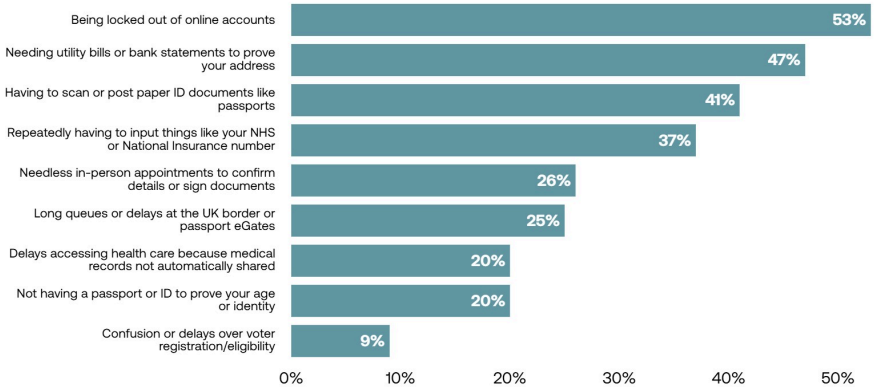
While there is a healthy debate to be had over the growing perception that "Britain is broken", the operating model of public-service delivery is undoubtedly under growing strain through a combination of tight fiscal constraints, failure demand (avoidable pressure from delays elsewhere in the system) and shifting demographics.[12] The price for this is paid by citizens.

When Britons interact with the state, it is often at life's pressure points: paying taxes, seeking care, applying for a licence or claiming support. Currently, the prevailing experience of this is of slow, fragmented and unnecessarily demanding processes: a tax on time that fuels avoidance, entrenches inequality and corrodes trust in institutions. The government estimates that the time burden of dealing with the state currently amounts, for an average citizen, to a week and a half every year.[13] The National Audit Office has estimated that customers spent the equivalent of 753 years waiting on hold for the Department for Work & Pensions (DWP) in 2023–24 alone.[14]

A word that very few people associate with government is "convenient". As our survey demonstrates, interactions are characterised by repetitive actions, requirements for a jumble of physical and digital documents, needless appointments and long queues.

FIGURE 9

Britons face many inconveniences when dealing with bureaucratic processes



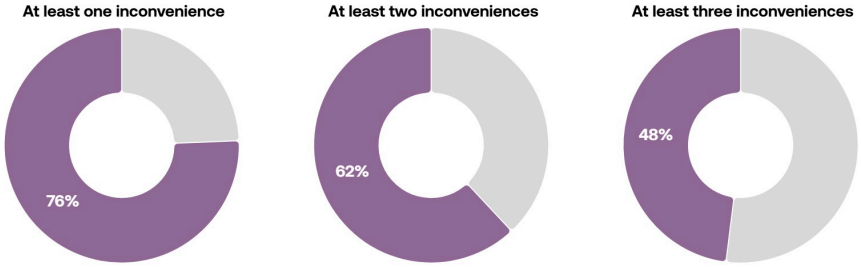
Q: Thinking about the last few years, can you say whether you have felt at all inconvenienced by any of the following?

Source: Yonder for TBI

At least 76 per cent of respondents cited at least one instance in which a simple, bureaucratic task felt inconvenient in the past few years – with just under half citing at least three instances.

FIGURE 10

Most respondents report facing more than one inconvenience when dealing with simple bureaucracy



Q. Thinking about the last few years, can you say whether you have felt at all inconvenienced by any of the following? Proportion of respondents that replied "yes" to at least one, two or three inconveniences.

Source: Yonder for TBI

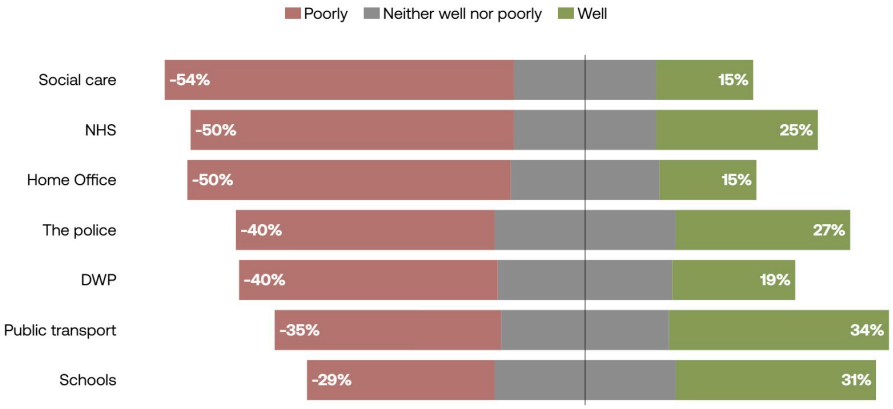
The scale of this burden is measurable across government.

The New Britain Project estimates that the average Briton loses between 28 and 41 minutes each week wrestling with inefficient public systems.[15] Across the adult population, this equates to 1.52 billion hours annually, often during working hours, since essential services such as GP bookings, council helplines and benefit queries are largely confined to the standard nine-to-five.

Public frustration with the quality of day-to-day interactions is reinforced by a broader sense that public services, even when accessed, are simply not functioning well. The prevailing perception is stark: most Britons believe social care, the NHS and the Home Office are underperforming, with dissatisfaction over the police, the DWP, public transport and schools also widespread. These are not isolated grievances, but symptoms of a system that feels slow, fragmented and unresponsive. Figure 11 illustrates how strongly this sentiment is reflected in public opinion.

FIGURE 11

Most people feel many key public services are not working well



Q: How well or poorly do you think the following public services are functioning?

Source: Yonder for TBI

Note: "Well" combines "Quite well" and "Very well," while "Poorly" combines "Quite poorly" and "Very poorly"; "Don't know" responses excluded.

Legacy, paper-heavy systems built on outdated processes and constrained resources inevitably generate backlogs that carry tangible costs for citizens. Despite increasing digitalisation, 31 per cent of driver-related transactions in 2021–22 were still fully or partially paper-based, including most licence applications involving medical conditions.[16] While online driver-related applications are typically processed within three working days, paper-based applications consistently lagged, with only eight of 30 months meeting the target of processing 90 per cent within ten working days.[17] In that context, the recent finding that 47 per cent of central-government services lack a digital pathway is damning.[18]

The lack of joined-up systems around citizens' interactions with different parts of the state creates an uneven experience that reflects poorly on government as a whole. Each department creates its own channels in isolation. Government functions in silos, drawing arbitrary boundaries across overlapping policy areas, leading to fragmented ownership and additional layers of bureaucracy. For citizens, this translates into disjointed services,

long waits and inconsistent outcomes – the everyday frustrations that create the impression of a dysfunctional state. The public does not see these failures as the fault of individual departments locked in mutual finger-pointing. Nor should it: what people experience is government failing as a whole and it is they who bear the consequences of the government's lack of coordination.

One of the government's flagship attempts to address this kind of fragmentation is GOV.UK One Login; a single credential that replaces multiple sign-in methods across central-government departments and allows citizens to prove their identity once and then reuse it across services. In principle, this should provide a secure entry point to government, creating a more coherent and consistent way for citizens to access services.

Yet progress has been limited. Despite One Login being created in 2021, by mid-2024 only 50 services had onboarded, with just over 3 million people registering an account. While around 6.2 million verified identities had been issued and the mobile app had been downloaded 8.8 million times, these figures partly reflect duplication and do not equate to active, unique users. Taken together, they still represent only a small fraction of the UK's 52 million adults, far short of the scale needed for universal adoption. This in itself illustrates the limitations of the current piecemeal approach.[19]

Many of the largest and most widely used government services remain outside the system, and some departments continue to operate their own logins and portals. This leaves citizens still navigating a patchwork of partial fixes, undermining the promise of a truly unified experience.

The weaknesses are structural. Without full departmental buy-in, clear accountability and rapid rollout, One Login risks becoming another layer added onto an already fragmented and bureaucratic system rather than the foundation of a coherent whole. For citizens, the effect is minimal: they still face multiple routes into government, repeated verification requests and the frustration of services that feel disconnected.

A universal digital-ID system, by contrast, would introduce a single touchpoint for most government services with a focus on fairness, control and convenience. This would cover use cases from identity verification to proof of age, address or eligibility, all through one user-friendly portal that reflects how citizens think of government (a single entity), rather than how government is organised (a collection of often autonomous bodies and departments).

To receive health care, secure housing or obtain benefits, citizens must from time to time demonstrate who they are and what is true about them. These checks fall into two categories:

- **Identity:** the fixed foundations of identity, including full name, date and place of birth, nationality or citizenship, biometrics and National Insurance number.
- **Attributes or credentials:** the facts that define circumstances and entitlements, including address and residency, immigration status, right to work, income and employment status, marital status, disability status, student status, qualifications and licences, voter eligibility and driving entitlements.

For the former, most citizens currently rely on a set of paper-based, government-issued documents, depending on the context:

- **Passport:** the primary standard for proving identity and nationality, used for international travel, right-to-work checks, tenancy agreements, banking and a range of public services.
- **Driving licence:** widely accepted as proof of both identity and address, and routinely required for opening bank accounts, age verification, renting property and certain licensing processes.
- **Birth certificate:** most often used when applying for passports, benefits or pensions, and as a fallback for children or those without photo ID.

These paper documents remain the backbone of identity and attribute verification, yet they are relics of a system designed for a pre-digital age. Because they often do not contain all the information necessary for the

specific context in which verification happens, they must be supplemented by even more paper documents – like the familiar "three months of bills" – and may even involve others "vouching" for the applicant.[20] The complexity of the system results in guidance on verifying identity that runs to almost 10,000 words.[21]

Static documents are being used to perform dual roles they cannot fulfil effectively. Passports, driving licences and birth certificates were created to establish fixed identity markers, but they are repeatedly repurposed to evidence attributes such as the right to work, the right to rent or entitlement to services.

The result is duplication across fragmented systems, with citizens asked to present the same documents again and again. This generates a self-perpetuating cycle of process and stress: access to services depends on proving both who you are and what is true about you, but doing so requires multiple stages of verification. In a system already characterised by long waits and broken processes, queues have become the default expectation. This creates a doom loop: citizens expect delays, so many avoid applying. Those who do apply often encounter complex, error-prone processes that deny them timely access to the services they are entitled to, reinforcing mistrust in the system.

Digital ID cuts through this chaos. TBI has long been the leading voice and standing advocate for digital ID, arguing in a series of papers that it can transform public services, drive economic growth and strengthen citizens' trust.

Digital ID should be understood as a foundational reform for governments struggling to make an outdated operating model work. It saves people time, reduces costs and provides the secure infrastructure needed to unlock innovation. TBI's economic analysis shows that, once implemented, a UK-wide digital ID could deliver a net improvement to the public finances of at least £2 billion annually through stronger identity verification. This figure is based on reducing benefit fraud by an estimated £1.25 billion each year,

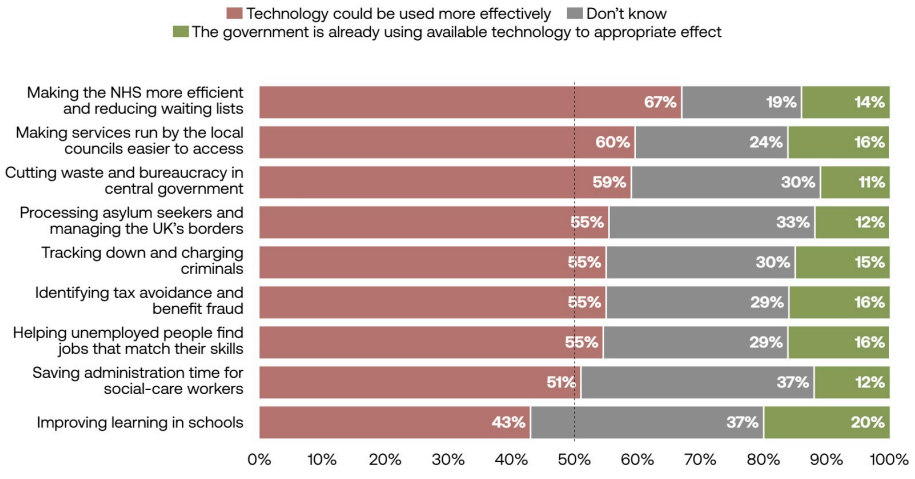
generating £0.6 billion in additional tax revenue and more accurately targeting crisis support, saving £0.2 billion annually. It does not account for wider benefits associated with digital ID.

As we set out in *The Economic Case for a UK Digital ID*, the estimated running costs are modest, around £100 million per year, and delivery within a single parliamentary term is achievable by building on the GOV.UK One Login programme.

There is clear public appetite for technology to help fix the issues plaguing public services. Two-thirds of respondents think NHS waiting lists could be reduced, 59 per cent think central-government waste could be decreased and 55 per cent think the processing of asylum seekers could be improved if technology were used more effectively. Improving outcomes through digitalisation is not only doable – it is popular.

FIGURE 12

There is strong support for the use of technology to improve public services



Q: Thinking about the following policy challenges facing the government: Do you think there is digital technology that could help tackle these issues but is not being fully used by the government at the moment – or do you think the government is already using digital technology to appropriate effect in these areas?

Source: Yonder for TBI

Digital ID's ability to streamline verification and join up information about a citizen is what makes it such a foundational element for genuine public-service reform.

Putting Privacy and Trust at the Heart of Digital ID

Many Britons already use various digital identity-verification systems in their lives – to apply for a credit card or loan online, set up insurance or even log in to gaming accounts. Recent research by the Department for Science, Innovation & Technology (DSIT) found that 44 per cent of respondents had used a digital identity-verification service at some point in their lives.[22] Those who reported using these kinds of services highlighted timesaving and convenience as the top benefits – with three-in-four respondents reporting faster transactions relative to the use of physical ID. Yet these benefits are not currently available to users of public services.

A government-run digital ID would change that, providing certainty around the identity and eligibility of service users while cutting bureaucracy and reducing the burden of interacting with the state. Success matters not only in terms of cost, but also in maintaining public confidence. Whether the purpose is to personalise services, hold key records such as a driving licence or simply provide a secure way to prove identity, more than eight in ten Britons believe a digital-ID system should be owned and operated by government.

FIGURE 13

Britons prefer government, not the private sector, to run multiple elements of a digital-ID system

Q: Advocates of a digital ID argue it would enable you to prove your identity, store key facts about yourself in a way that is convenient and secure, and help you more easily access a broad range of public and private digital services. For each of the following things, would you prefer them to be run by the government or run by private-sector companies?
1. A digital ID that allows you to prove you are who you say you are
2. A digital ID that holds key details about you, such as your qualifications or that you have a driving licence
3. A digital ID that can personalise government services, for example through an app on your phone

Source: Yonder for TBI

Yet the Data (Use and Access) Act 2025 sets out a framework in which private providers take on much of the delivery. Public opinion suggests a different balance: people want government firmly in charge. This does not preclude opportunities for the UK's well-established digital-verification industry to add value by innovating on core functionality, but aligning the system with this expectation is essential to securing public trust and widespread adoption.

FIGURE 14

People want privacy, security and user controls embedded in digital ID

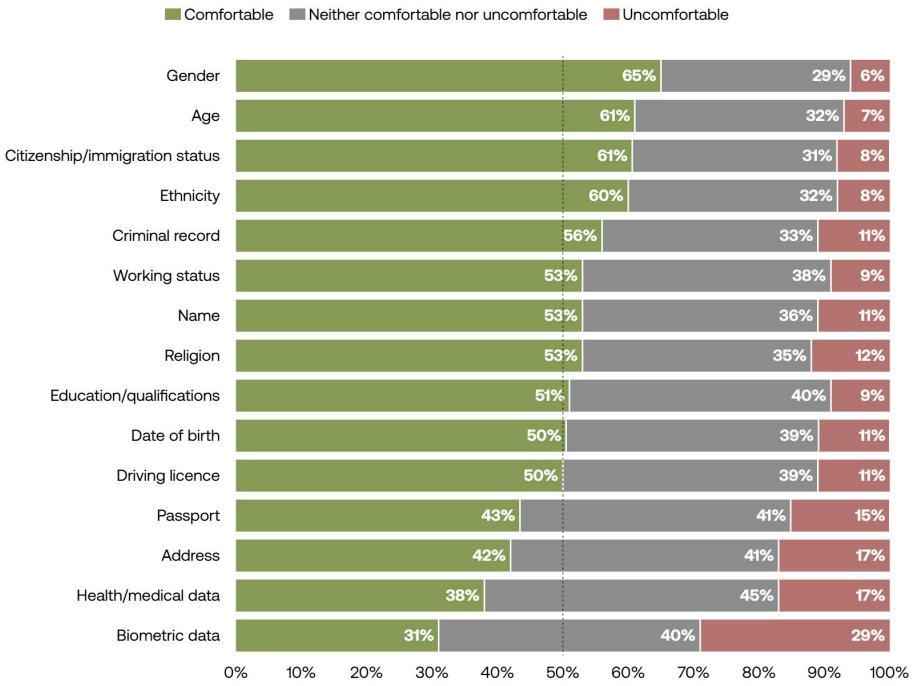
Q: If a digital-ID system were to be introduced, please rank each of the following in terms of how important you think they would be to include as part of the system, where 1 is the most important and 8 is the least important. Percentage represents the proportion of respondents who ranked each option in their top three.

Source: Yonder for TBI (March 2024)

The public's top priority is strict data-security measures, with 61 per cent of respondents identifying these as essential. This is followed by limited access, with 57 per cent wanting only relevant bodies to use their information. A further 40 per cent stress the importance of user controls, allowing individuals to decide what data are shared and with whom. Taken together, these priorities make clear that any system must be built to protect citizens, placing control firmly in their hands while guarding against misuse.

FIGURE 15

People are more comfortable with the government having access to some types of personal information than others



Q: How comfortable would you be with the government having access to each of the following forms of your personal information in order to do this? Please use a scale of 0-10, where 0 means you would be very uncomfortable and 10 means you would be very comfortable.

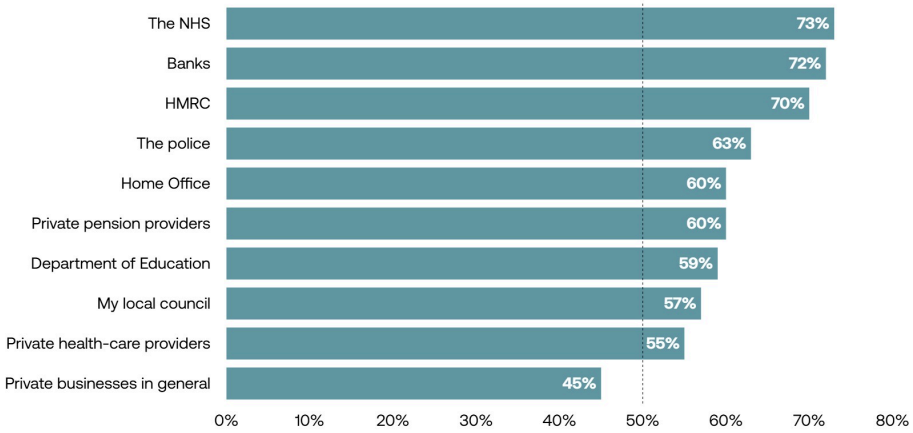
Source: Yonder for TBI (March 2024)

Public trust is the foundation for government taking on a central role in digital-ID delivery. Overall, the public leans towards supporting broad data-sharing with government but, consistent with recent Ipsos findings, biometric data remain the area of greatest hesitation.[23]

Britons also favour public institutions over the private sector when it comes to data protection: 73 per cent trust the NHS to safeguard their data, compared with 55 per cent for private health-care providers and just 45 per cent for private businesses overall.

FIGURE 16

When it comes to data protection, Britons trust government institutions over the private sector



Q: To what extent, if at all, do you think the following bodies/organisations can be trusted to hold and use personal data safely and securely? Net per cent believing very much/to some extent.

Source: Yonder for TBI

The government should lead on digital ID with transparency and accountability, designing a system that puts citizens first, and is built on fairness, control and convenience.

Such a model would build on this reservoir of trust, making digital ID a public good rather than a commercial product. The private sector still has an important role to play, offering innovation, technology and added services – but this should be within an interoperable framework that is clearly owned and directed by government. By putting central government in the lead, digital ID can both protect citizens' data and tackle cumbersome bureaucracy, delivering faster, simpler and better services across a wide range of functions.

The experiences of other countries show that systems of this kind are more secure and better for citizens' privacy than the existing approach. Identity fraud becomes significantly more difficult; instead of forging a paper

passport or using social engineering (manipulating people to reveal sensitive information) to bypass imperfect identity-verification systems, criminal networks would be confronted with strong encryption and repeated, stringent biometric checks of the kind that protect bank accounts from unauthorised access.[24]

Similarly, the risks to privacy from digital ID are significantly lower than the current status quo. Digital-ID systems rely on secure, constantly monitored data pipelines to exchange data. This minimises opportunities for unauthorised data-sharing, either maliciously or by mistake. Prominent data breaches, such as the 2022 Afghan data leak, illustrate the dangers of the current ad-hoc data-sharing model. This leak resulted from a Ministry of Defence official accidentally emailing an unencrypted spreadsheet with sensitive personal details of up to 100,000 individuals, putting lives at risk.[25]

Digital ID, by contrast, can be set up to limit access to sensitive information and minimise "data leakage". For example, through selective disclosure citizens can choose what information to share with others and when. Shared data can be minimised to only what is strictly necessary – for example, instead of sharing a full date of birth to prove someone's age, digital ID can simply confirm if the citizen is older or younger than 18.

As for the common argument that digital ID represents a threat to civil liberties, evidence suggests there is little truth to it. Across liberal democracies comparable to the UK, the introduction of digital ID has not led to a drift into authoritarianism that critics routinely predict. Many countries with mature, widely-used digital-ID systems rank highly in terms of democratic performance.

In the Freedom House Freedom in the World index, Estonia, which introduced digital ID in 2002 and has close to 100 per cent take-up, scores 96/100 (up from 94 in 2017).[26] Portugal, which launched electronic identity in 2007 and a mobile solution in 2014, also scores 96/100.[27] Western Europe as a whole, where digital-ID wallets are being introduced as part of a European Union-wide mandate, bucked the trend of democratic decline in the latest

issue of the Economist Intelligence Unit Democracy Index, with the highest score of any region.[28] Norway and Sweden, ranked first and third in the world respectively, both have widely used digital IDs.[29]

This demonstrates that, by itself, the introduction of digital ID does not lead to an erosion of civil liberties. Academic research suggests that greater digitalisation is neither a necessary nor a sufficient condition for greater repression – what matters is whether a history of repression exists already.[30]

The UK ranks highly among the world's democracies, placing 17th globally in the Democracy Index, providing a strong cultural and institutional backstop against a slide into totalitarianism.[31] In that, it is similar to other liberal democracies with a Westminster system of government. In fact, one argument made recently by critics of digital ID is that Europe is not a relevant comparison for the UK, with countries such as New Zealand (ranked second in the 2024 Democracy Index) and Australia (ranked 11th) a closer match in terms of culture and the political system.[32] It is notable, therefore, that both of those are currently in the process of introducing their own versions of digital ID.[33,34]

In *The Great Enabler: Transforming the Future of Britain's Public Services Through Digital Identity*, TBI set out three core principles that must underpin a trusted, government-owned digital ID:

- **Transparency and individual control.** Public trust depends on people having visibility of and control over their data. A system that shows when, why and by whom records are accessed, and limits disclosure to only what is necessary, would reassure citizens and make digital ID more secure than physical documents.
- **Security and robust privacy protections.** The system must avoid a centralised database vulnerable to leaks and instead adopt a decentralised model, using encryption, one-time tokens and biometrics to safeguard privacy and protect against identity theft.

- **Speed and utility.** Digital ID should simplify everyday life, working across both public and private services, from accessing benefits to renting a car or verifying age online, and it must be inclusive, ensuring access for those without smartphones. But whether accessed through a smartphone or fallback channels, the ID would be always available and always up to date, replacing a fragmented, paper-dependent system with a single universal approach.

A well-designed, government-owned digital ID offers a practical route to reform, cutting bureaucracy, strengthening security and creating a single, convenient gateway to the state. International experience shows these systems can be delivered securely, without eroding democratic values, and with clear benefits for citizens. Digital ID would make services easier to access, save money through reduced fraud and administrative costs, and underpin a more efficient state. For a government seeking fiscal discipline and better outcomes, it is a foundational reform, modernising public services, restoring trust and providing the basis for a new, citizen-centred model of delivery.

Launching a New Model of Public Services

As we set out in *Governing in the Age of AI: A New Model to Transform the State*, the current operating model of public-service delivery – slow, unscalable, increasingly expensive – is no longer sustainable. The government has rightly recognised the potential of new technologies, and AI in particular, to transform the fortunes of our public sector alongside the wider economy.[35] AI can enable a new model of public services: personalised, always-on, data-driven.

Digital ID is both the foundational infrastructure and the front door to the delivery of these services. As TBI has set out in a series of papers, it would put patients in control of their health care and unlock a new approach to personalised prevention. It would give teachers unprecedented insight into the needs of learners and drive a shift to continuous improvement across

the system, reversing and closing the disadvantage gap. In welfare, it would help claimants find and enter fulfilling careers, not just any job at any cost, improving lives and growing the economy.

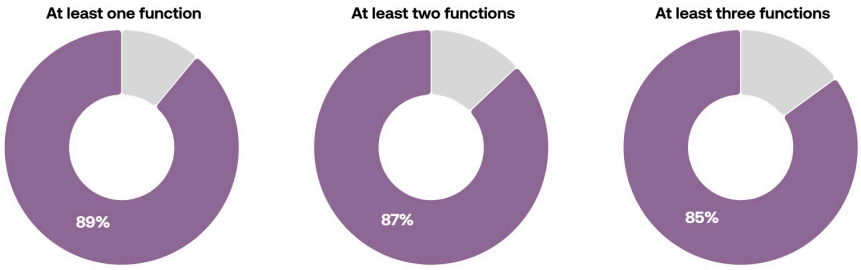
Some of the most ambitious departments have begun to explore what this shift looks like. The NHS 10 Year Plan for England has committed to a digital health record that would help build a full picture of information held about a patient across the system.[36] The Ministry of Justice's AI Action Plan for Justice has committed to introducing a single, consistent offender ID to reduce administrative burdens, support better decision-making and improve rehabilitation outcomes.[37] DSIT has launched a beta version of a GOV.UK app that is intended to hold digital credentials, with ambitious plans to include data from across the public sector over the next few years.[38,39]

To unleash the full benefits of a universal digital-ID system, these initiatives need to work together. A key step towards this is to lift the ambition of the GOV.UK app from a holding place for credentials to a secure gateway and single front-door to essential services and transactions.

When asked for their views on a digital ID that could personalise government services through a mobile app, more than eight in ten Britons wanted to see at least three of the potential functions we described included. This shows clear appetite for a comprehensive system that could transform the way people access services.

FIGURE 17

Respondents want a digital-ID app to combine a range of features



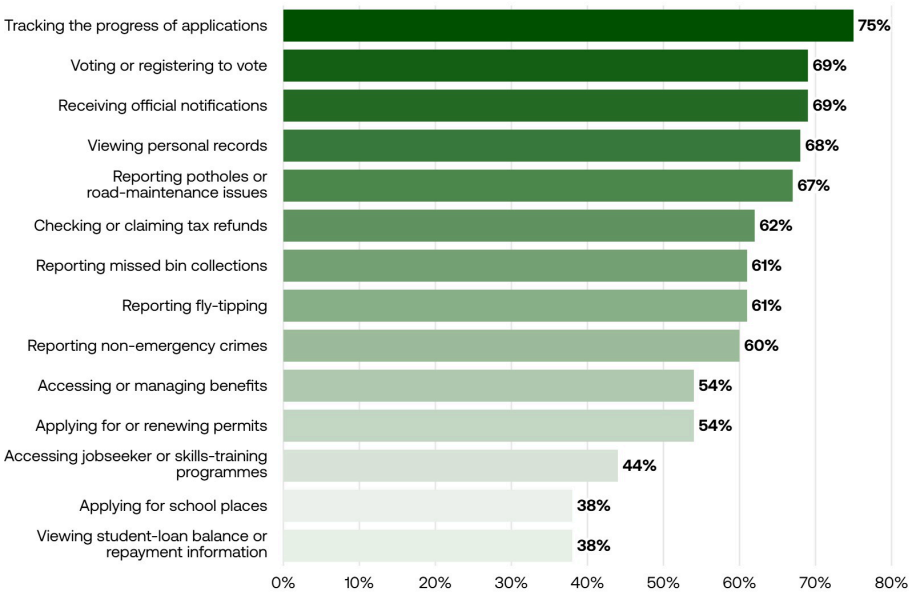
Q: Some are suggesting the government should introduce a new app, allowing instant access to a range of public services. For each of the following features, can you say whether you would or would not want the function to be included if such an app were introduced?
Proportion of respondents that replied "I would want this function included" to at least one, two or three functions.

Source: Yonder for TBI

The opportunity is squarely with government. Delivering a well-designed, intuitive digital-ID system that unlocks a wide range of everyday applications would quickly prove its value and cement public trust.

FIGURE 18

Many potential functions enjoy majority support, with civic-engagement and proof-of-identity tasks among the most popular



Q: Some are suggesting the government should introduce a new app, allowing instant access to a range of public services. For each of the following features, can you say whether you would or would not want the function to be included if such an app were introduced? Proportion of respondents that replied "I would want this function included".

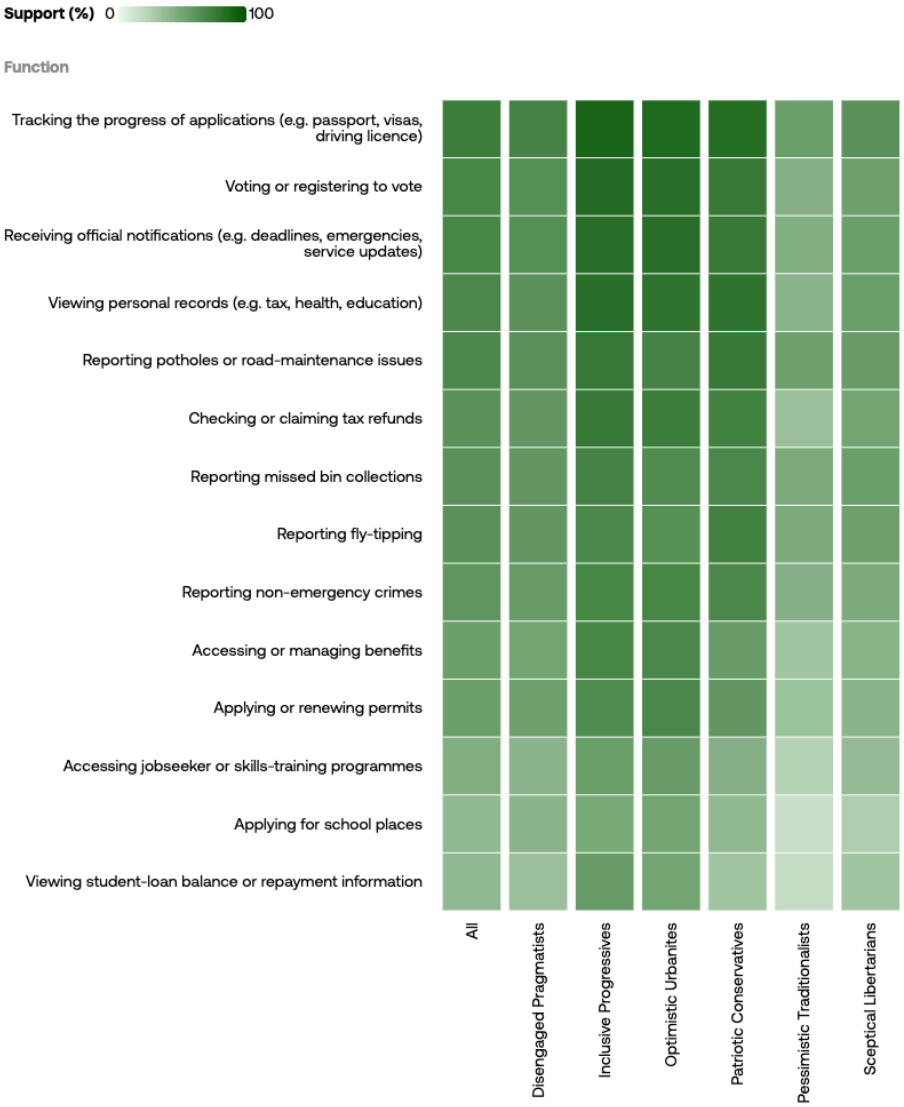
Source: Yonder for TBI

Three-quarters of respondents want the ability to track the progress of their applications, and over two-thirds want to view personal records and vote online. Similarly welcomed features pertain to Britons' interactions with local services; reporting road-maintenance issues, fly-tipping, missed bin collections and non-emergency crime.

When these functions are mapped to our digital-ID segments of the British public, clear patterns emerge around which digital services command broad support.

FIGURE 19

Functions related to civic engagement attract support across our six segments



Q: Some are suggesting the government should introduce a new app, allowing instant access to a range of public services. For each of the following features, can you say whether you would or would not want the function to be included if such an app were introduced? Proportion of respondents that replied "I would want this function included".

Source: Yonder for TBI

Use cases tied to civic engagement and identity – the ability to track applications, vote or register to vote, and view personal records – consistently stand out as the most popular. These can be understood as the "core" functions of any future mobile app: simple, high-impact interactions with the state that people across the political spectrum want to see digitalised, even among the segments most sceptical of digital ID.

Drilling down further, it is possible to see which features are most likely to appeal to those with lower initial support for digital ID. Looking more closely at the groups most resistant to digital ID – the Sceptical Libertarians and Pessimistic Traditionalists – a clear pattern emerges. Their support grows around tangible, everyday services that demonstrate visible value. For instance, 56 per cent of Sceptical Libertarians and 52 per cent of Pessimistic Traditionalists express support for functions such as reporting potholes and road-maintenance issues. Integrating this functionality – as opposed to the current postcode-lottery of council websites – into a universal, easy-to-access app that is linked to the citizen's "home" council and allows for quick updates on progress around addressing issues would add further value to a digital-ID system.

These could be seen as modest services. However, they show how digital delivery can break through entrenched frustrations – solving practical problems in ways people feel directly, in their communities and in their daily lives. Digital ID can become the solution to the dozens of little annoyances that plague people's everyday interactions with government – from remembering when and where to vote to calling a dozen agencies to update their address or repeatedly filling in the same forms. It can also serve as a channel for proactive communications from public bodies to citizens, such as updates on the progress of applications, crime reports or requests to fix potholes. This raises the stakes on delivery, incentivising the state to act, and provides an upside – swift action will not go unnoticed.

USE CASES

Life With a Digital ID Is Easier and More Convenient

VIEWING RECORDS

A citizen logs on to the digital-ID app with a quick biometric check, just like when they open their phone or banking app. On the main screen, they can see their information and any updates to it, so if any of the details are wrong, they can see this and act on it. If they move, they only need change their address once, because the update cascades across the system – changing the address on their driving licence, informing the local council, tax authorities and the GP practice, suggesting an update to the electoral roll and so on. Any messages for them – for example, from HMRC to let them know of a tax refund, or from their GP about an appointment that has been moved – are visible in the app, so there is no need for a paper letter unless they explicitly ask for one.

VOTING

A prospective eligible voter confirms their pre-filled information in the digital-ID app. If they move house, their voting registration can be automatically updated. On election day, they receive a notification: "Polls are open from 7am to 10pm. Your polling station is at this address. Click here to get directions." At the station itself, a quick scan of the app confirms the voter's identity – so they don't need to work out what kind of ID to bring, out of a long list of options, to avoid being turned away.[40] Once the polls close, the app enables them to track the count for their ward or constituency in real time.

REPORTING POTHOLES OR FLY-TIPPING

A resident opens up their digital-ID app and snaps a photo of a pothole they spot on the street. The report, with the exact location attached, is immediately sent to the responsible council. The council comes back with an update: "Repair scheduled for Friday". On the day, a follow-up comes: "Repairs completed. Thank you for your report!", complete with a photo. If there's a delay, the app says so. It's as simple as tracking a package delivery.

RECEIVING CHILD BENEFIT

As soon as a birth is registered, the parents' digital IDs are updated with the newborn's name, NHS number and other relevant information. For parents who earn less than the threshold, a message pop ups in the app to inform them that they are eligible for child benefit. After a few quick questions to decide which parent receives the benefit and which bank account to use, the first payment can be made – there is no need to make a separate claim. As the child gets older, the app keeps up with relevant updates (to the parents' income through HMRC or to their marital status) and payments are adjusted or reallocated automatically until the child ages out.

Digital ID is an example of a disruptive-delivery agenda that demonstrates how government can be made faster, simpler and more effective. Digital ID is not just a technical fix – it is a platform for empowerment. It can cut through bureaucracy, make services seamless and show that government is once again on the side of the citizen.

Clearly, part of digital ID's appeal lies in the breadth of applications it can bring together under a single system. Community-facing functions enjoy broad, cross-generational support, while uses linked to welfare and education are particularly valued by those of working age and students.

A successful national app should anchor itself in the core, consensus functions that enjoy support across all groups, while layering on practical, everyday services that help to build trust among sceptics. This approach balances breadth with pragmatism, maximising both uptake and legitimacy across the public. For more complex areas of public-service delivery, such as health care, dedicated apps such as the NHS App can and should continue, with the digital ID serving as a jumping-off point – alerting citizens to any new information or messages, providing links to key functionality and then securely transferring them to the right place in the dedicated app.

Digital ID offers more than faster services; it can enable a smarter state that knows when and how to help, without citizens having to ask. By confirming identity and linking verified attributes, such as income level, disability status, household composition or immigration status, a digital ID can enable government to act proactively on what it lawfully knows to be true. This creates the potential for proactive service delivery: for example, automatically notifying and offering a council-tax reduction to an eligible household because verified data already demonstrate its occupants meet statutory criteria. The ability to suggest and deliver services based on what is known about a citizen and their needs is foundational to the AI-enabled state and its enormous productivity benefits, which we estimate at £40 billion a year – an assessment closely matched by the government's own analysis.[41]

Unlocking the promise of a universal digital ID – fairness, control and convenience – will rest on the state's ability to successfully implement a complex IT project. This requires the government to couple best practice for building digital products with relentless attention to delivery.

04

Implementing a Digital-ID System That Works

Digital ID must be treated as a national priority. Its implementation cannot follow in the footsteps of previous failed government IT projects and therefore should not be allowed to proceed by default; it should instead become the model for digital delivery of a new generation of services. Such a crucial piece of government instruction cannot be left to the private sector to own. The Prime Minister's Office must designate digital ID as a key project, with a delivery unit tracking progress and intervening at the first sign of delay or overrun.

Digital ID Should Be an Exemplar Digital Project

TBI has previously estimated, in line with other government projects, that establishing the enabling infrastructure for a UK-wide digital ID would require an upfront investment of around £1 billion, with ongoing annual running costs of approximately £100 million. The £1 billion setup cost would fund large-scale enrolment as well as the development of the core digital infrastructure needed to link data securely across government departments, providing the foundation for a system that is both scalable and resilient.

Much of this work is already underway as part of the One Login rollout and DSIT's Blueprint for Modern Digital Government, so the overall cost is likely to be lower. For example, Labour Together estimates the cost of delivering a digital right-to-work/right-to-rent credential, including the GOV.UK app, at between £140 and £400 million.[42]

The government already has the foundations in place; GOV.UK One Login provides the technical base on which to build. Yet the system remains underused, because the ambition has not followed. What is missing is full political will and departmental buy-in.

Without central leadership, the implementation of digital ID risks becoming another HS2, a project ambitious in promise but paralysed by drift, indecision and delay, resulting in large parts of the route scrapped and the public left questioning its value. What should have been a transformative investment in national infrastructure has instead become, in the words of the transport secretary, "an appalling mess".[43]

Digital ID cannot follow this path; it must show what is possible when political will is matched with discipline in delivery. As a primarily digital project, its implementation needs to be led by a highly technical and multidisciplinary team, melding cross-Whitehall expertise with user research and a strong engineering and cyber-security core. The team needs to be hired on the basis of technical interviews rather than traditional civil-service recruitment questions, and this process cannot be allowed to drag on the way recruitment for the Incubator for AI has.[44,45] Pay should follow private-sector benchmarks to ensure the best possible talent pipeline.

To support integration efforts across departments, a forward-deployed engineer model should be used, in which team members are embedded with departmental digital teams and customers, and are empowered to rapidly build prototypes.[46] Instead of an upfront allocation, funding for the programme should follow the best practice laid out in the recent Performance Review of Digital Spend, with a step-by-step approach that unlocks new funds based on milestones and allows for rapid iteration and experimentation.[47]

The government already has examples of successful digital-transformation projects delivered at pace, such as the improvements made to the Passport Office in the wake of massive post-Covid backlogs.[48] Digital ID should become another such example.

Delivery Should Be Prioritised by the Prime Minister's Office

Digital ID will only succeed if government proves it has the political will to lead and the discipline to deliver in the public interest. This requires treating digital ID as a No 10 priority. A dedicated team within the Prime Minister's Office, the Digital-ID Delivery Unit (DIDU), should be established to track progress relentlessly and resolve obstacles in real time. DIDU must have unambiguous political sponsorship, a focused remit, high-calibre leadership and undergo regular stocktakes to unblock issues.

DIDU needs a small team with mixed expertise in policy, service design, digital delivery and data to push, unblock and drive progress. An accountable leader – responsible for delivery, providing regular updates on progress, and maintaining public confidence through consistent communication and visible defence of the project – should be appointed as the public face of the programme, as recently proposed by Labour Together.[49] This individual should report directly to the prime minister each week, ensuring the centre of government retains clear sight of performance and emerging risks.

DIDU must hold departments to account. Its authority should rest on three foundations. First, transparency: by publishing clear dashboards and progress data, DIDU can make visible which departments are meeting commitments and which are lagging, creating political and peer pressure in the same way performance league tables have in other parts of government.[50]

Second, spending control: DIDU should maintain the right to link approval of digital expenditure and release of transformation funds to departments demonstrating tangible progress, building on the Cabinet Office's existing digital and technology spend-control framework. This should follow an "earned autonomy" model – departments that show they are able to integrate at pace should be left to proceed, while those lagging behind may

need a stronger intervention to enforce a government equivalent of a “Bezos mandate” (a requirement that all public-sector data must be made interoperable).[51]

Third, accountability through leadership: digital-ID milestones should be embedded in the objectives of permanent secretaries and directors general, with progress fed into ministerial scorecards reviewed at the centre, giving the prime minister and the chancellor of the Duchy of Lancaster direct visibility of blockers.

The starting point for digital ID should be universality. No 10 and DIDU should start by mandating that every citizen is issued with a One Login at the age of 18, making it the default gateway to public services. This universality is essential: without it, adoption will continue to remain piecemeal and fragmented. All departments must therefore be required to integrate their services with One Login, ensuring that citizens can use a single identity across government.

To enforce this, DIDU should set immovable deadlines for retiring legacy login systems and escalate any missed commitments directly to ministers. Non-compliance must trigger real consequences, whether through the suspension of funding approvals, public naming via performance data or escalation to the prime minister. Where departments obstruct progress, DIDU must have the authority to reassign delivery capacity or provide a surge of technical and policy resource from the centre of government to accelerate progress.

With universal issuance as the anchor, DIDU can evolve into the engine of system-wide change, embedding digital ID across the whole of government. Over time, the digital-ID infrastructure should become the only way to prove one’s identity in interacting with government. This is not the same as forcing everyone to carry a smartphone – global experience shows that digital-ID fallback schemes, which provide citizens with alternative means of accessing the cloud infrastructure that is used for verification, can effectively ensure inclusion. In India, for example, voice interfaces for digital-ID-enabled financial transactions help a large segment of the population without literacy skills to fully participate in the economy.[52]

The success of digital ID depends on benefit to citizens being embedded in its core, anchored in the principles of fairness, control and convenience. Delivery must be sequenced yet visible, ensuring progress is both manageable and demonstrable. An iterative, test-and-learn approach is essential to embedding these principles, allowing government to build confidence and capability while avoiding the pitfalls of large, one-off programmes. A phased rollout, beginning with sectors where identity verification is already standard practice, offers the opportunity to deliver rapid, tangible impact.

The Home Office is the natural starting point: integrating digital ID into areas such as passports, visas and immigration status, where secure identity checks are already routine, would provide early proof of concept while visibly advancing fairness, control and convenience.

However, the Home Office should only be the start. Once established, the system should quickly expand to HMRC and DWP, where a single verified identity could simultaneously reduce fraud and simplify life for citizens managing tax and welfare claims, and integrate with the NHS App. Local councils should be supported to integrate with digital ID and its associated app to create a Local Navigation Assistant experience (as described in *Governing in the Age of AI: Reimagining Local Government*), with common tasks – such as reporting potholes or finding out the day of bin collections – following a set pattern no matter where a citizen lives.

Each stage of implementation must demonstrate real improvements for users, generate evidence of value and inform the design of the next phase, ensuring that progress is cumulative, credible and firmly grounded in public benefit.[53]

Conclusion

Britain is calling for a state that works. A universal digital ID is foundational to that ambition. It will help people prove who they are, sharing only what is necessary, and allow them to access services quickly and securely. The public is ready. Support spans the political spectrum, reflecting tangible benefits: reduced fraud, streamlined bureaucracy, quicker decision-making and fairer outcomes.

Digital ID is the infrastructure of a modern state: secure, citizen-controlled, resilient. Selective disclosure, biometrics and audit trails make it more private than paper. International comparators show it can be delivered without compromising freedoms. TBI polling shows people want government to lead.

Digital ID narrows the space for traffickers and rogue employers. It reduces errors, closes loopholes and restores confidence that rules are enforced fairly. It also removes the everyday frictions that feed cynicism, by allowing users to prove eligibility once, track applications in real time and report issues without queues or confusion.

But delivery is the test. This must not become another HS2. Digital ID must be treated as a flagship national project. That means a mandate from No 10, a dedicated delivery unit, an engineering-led team and funding tied to milestones, not guesswork.

Universality matters. Every resident should be issued One Login credentials, with legacy logins retired. Fallbacks must be in place for those without smartphones. And ultimately the experience of dealing with the state is what matters most – make the system easy to use and citizens will respond.

Digital ID is not a silver bullet – but it is common sense. The outcome is a state rebuilt on fairness, control and convenience. A single front door to government, matching how people live their lives. Time saved. Costs cut. Trust restored. Voters will back those who deliver. A modern digital ID, done right, is the clearest signal that government can deliver.

Methodology

Foundational qualitative research

Yonder conducted six in-person focus groups on behalf of the Tony Blair Institute for Global Change in December 2023. The groups consisted of adults (aged 25+) and were held in London, Newport and Rugby. Groups were split by age (44 and below/45+) and included participants who had very low digital skills. The discussions lasted 90 minutes and were moderated by experienced Yonder researchers, based on a discussion guide developed by Yonder in collaboration with TBI.

Quantitative research

Yonder interviewed 4,008 UK adults online between 24 and 26 March 2024. Polling covered the whole of the UK and data were weighted to be representative of the whole population by gender, age, region and socioeconomic group.

Attitudinal segmentation

Poll data were analysed to create an attitudinal segmentation of the UK public on the basis of their attitudes to digital ID. This identified six discrete attitudinal groups with coherent views on issues relating to the adoption and use of digital ID.

Updated polling

Yonder interviewed 2,014 UK adults online on 23 and 24 June 2025. Polling covered the whole of the UK and data were weighted to be representative of the whole population by gender, age, region and socioeconomic group. The poll included an algorithm to allocate respondents to the identified attitudinal segments.

The full data can be found here.

Endnotes

1 https://www.thetimes.com/uk/politics/article/digital-id-cards-crime-justice-commission-hcvbxfj57

2 https://www.ipsos.com/en-uk/57-britons-support-national-id-card-scheme-have-significant-concerns-over-data-security-and

3 https://www.youtube.com/watch?v=3mzCVRdcAUM

4 https://www.telegraph.co.uk/news/2023/09/03/people-smugglers-sell-fake-passports-instagram-stories/?msockid=2ec7474d5cfd60e7188b537c5dc561cd

5 https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/tax/documents/ey-gl-shadow-economy-report-02-2025.pdf

6 https://migrationobservatory.ox.ac.uk/resources/briefings/unauthorised-migration-in-the-uk/

7 https://www.gov.uk/government/publications/employer-awareness-of-right-to-work-checks/employer-awareness-of-and-self-reported-compliance-with-right-to-work-checks

8 https://www.gov.uk/government/publications/returns-from-the-uk-and-illegal-working-activity-since-july-2024/illegal-working-activity-between-5-july-2024-to-31-may-2025

9 https://www.gov.uk/government/publications/returns-from-the-uk-and-illegal-working-activity-since-july-2024/illegal-working-activity-from-5-july-2024-to-22-march-2025

10 https://www.thetimes.com/uk/crime/article/people-smugglers-migrants-small-boat-crossing-package-deals-znvr080b6

11 https://static1.squarespace.com/static/64f707cf512076037f612f60/t/6841899eee8b0741ea8756a7/1749125534854/Final%5FBritCard%5FLabour+Together.pdf

12 https://samf.substack.com/p/britain-isnt-broken

13 https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review

14 https://www.nao.org.uk/wp-content/uploads/2024/07/dwp-customer-service-summary.pdf

15 https://www.newbritain.org.uk/%5Ffiles/ugd/8be189%5F5e20b1987ed8444c913dafa34af0a407.pdf

16 https://www.nao.org.uk/wp-content/uploads/2022/11/backlogs-in-driving-licence-applications-summary.pdf

17 https://www.nao.org.uk/wp-content/uploads/2022/11/backlogs-in-driving-licence-applications-summary.pdf

18 https://www.gov.uk/government/publications/state-of-digital-government-review/state-of-digital-government-review#services

19 https://gds.blog.gov.uk/2024/11/12/gov-uk-one-login-celebrating-50-services/

20 https://www.gov.uk/government/publications/how-to-accept-a-vouch-as-evidence-of-someones-identity

21 https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual/how-to-prove-and-verify-someones-identity

22 https://www.gov.uk/government/publications/digital-identity-sectoral-analysis-report-2025/digital-identity-sectoral-analysis-2025?utm%5Fsource=chatgpt.com

23 https://www.ipsos.com/en-uk/57-britons-support-national-id-card-scheme-have-significant-concerns-over-data-security-and

24 https://cyberandspecialistoperationscommand.blog.gov.uk/2022/11/09/one-click-is-all-it-takes-social-engineering/

25 https://www.theguardian.com/uk-news/2025/sep/03/afghans-resettled-uk-mod-data-leak-report-national-audit-office

26 https://freedomhouse.org/country/estonia/freedom-world/2025

27 https://freedomhouse.org/country/portugal/freedom-world/2025

28 https://www.eiu.com/n/democracy-index-2024

29 https://www.economist.com/interactive/democracy-index-2024

30 https://onlinelibrary.wiley.com/doi/10.1111/spsr.12607

31 https://www.economist.com/interactive/democracy-index-2024

32 https://bigbrotherwatch.org.uk/wp-content/uploads/2025/09/Checkpoint-Britain.pdf

33 https://my.gov.au/en/about/help/digital-id

34 https://www.dia.govt.nz/Digital-Identity-Services

35 https://www.gov.uk/government/publications/ai-opportunities-action-plan/ai-opportunities-action-plan

36 https://www.gov.uk/government/publications/10-year-health-plan-for-england-fit-for-the-future

37 https://www.gov.uk/government/publications/ai-action-plan-for-justice/ai-action-plan-for-justice

38 https://www.gov.uk/guidance/using-govuk-wallet-in-government

39 https://www.gov.uk/government/publications/a-blueprint-for-modern-digital-government/a-blueprint-for-modern-digital-government-html

40 https://www.electoralcommission.org.uk/voting-and-elections/voter-id/accepted-forms-photo-id

41 https://committees.parliament.uk/publications/47602/documents/248450/default/

42 https://static1.squarespace.com/static/64f707cf512076037f612f60/t/6841899eee8b0741ea8756a7/1749125534854/Final%5FBritCard%5FLabour+Together.pdf

43 https://www.theguardian.com/business/live/2025/jun/18/uk-inflation-expected-dipped-may-federal-reserve-interest-rates-oil-business-live

44 https://committees.parliament.uk/oralevidence/15623/html/

45 https://www.ft.com/content/a47b71a5-dca1-439d-8a0c-e18d6b0d1df3

46 https://maxdauber.substack.com/p/forward-deployed-engineer-profession

47 https://assets.publishing.service.gov.uk/media/67ceb0a4df9470296491605a/Performance%5FReview%5Fof%5FDigital%5FSpend%5F-%5Ffor%5Fpublication%5Ffinal%5Fversion.pdf

48 https://www.thetimes.com/uk/article/passports-in-just-five-days-how-a-broken-system-was-fixed-bpn8jvnsq

49 https://static1.squarespace.com/static/64f707cf512076037f612f60/t/6841899eee8b0741ea8756a7/1749125534854/Final%5FBritCard%5FLabour+Together.pdf

50 https://www.gov.uk/government/publications/a-blueprint-for-modern-digital-government/a-blueprint-for-modern-digital-government-html

51 https://nordicapis.com/the-bezos-api-mandate-amazons-manifesto-for-externalization/

52 https://www.wsj.com/world/india/in-indias-mobile-payments-boom-even-beggars-get-qr-codes-11653653383

53 https://d1rnadml6vbx0i.cloudfront.net/Public-Digital%5FThe-Radical-How.pdf

TONY BLAIR
INSTITUTE FOR
GLOBAL CHANGE

Follow us

facebook.com/instituteglobal

x.com/instituteGC

instagram.com/institutegc

General enquiries

info@institute.global