DEMOS

DEFINING DIGITAL ID

IDEATING A PEOPLE CENTRED AND TECH POSITIVE APPROACH TO DIGITAL ID IN THE UK

WORKSHOP SUMMARY

ELIZABETH SEGER
POLLY CURTIS
ALEXANDER IOSAD
COSMINA DOROBANTU
ALEXANDER EVANS

JANUARY 2026

Published by Demos January 2026

15 Whitehall, London, SW1A 2DD
T: 020 3878 3955
hello@demos.co.uk
www.demos.co.uk

ABOUT THIS PAPER

This briefing paper is the summary of a workshop examining the key opportunities and challenges for a digital identification program in the UK. It was held in partnership between **Demos**, the **Tony Blair Institute** and the **LSE** with input from the Department of Science, Innovation and Technology, and the Cabinet Office. It was attended by a diverse range of civil society organisations.

It is part of Demos's work focused on achieving more ***Trustworthy Technology***, in which technological progress aligns with the needs and values of citizens. It will also inform our future work on ***Public Service Reform***, which makes the case for data, digital and technology to be deployed in service of more relational and effective public services.

CONTEXT

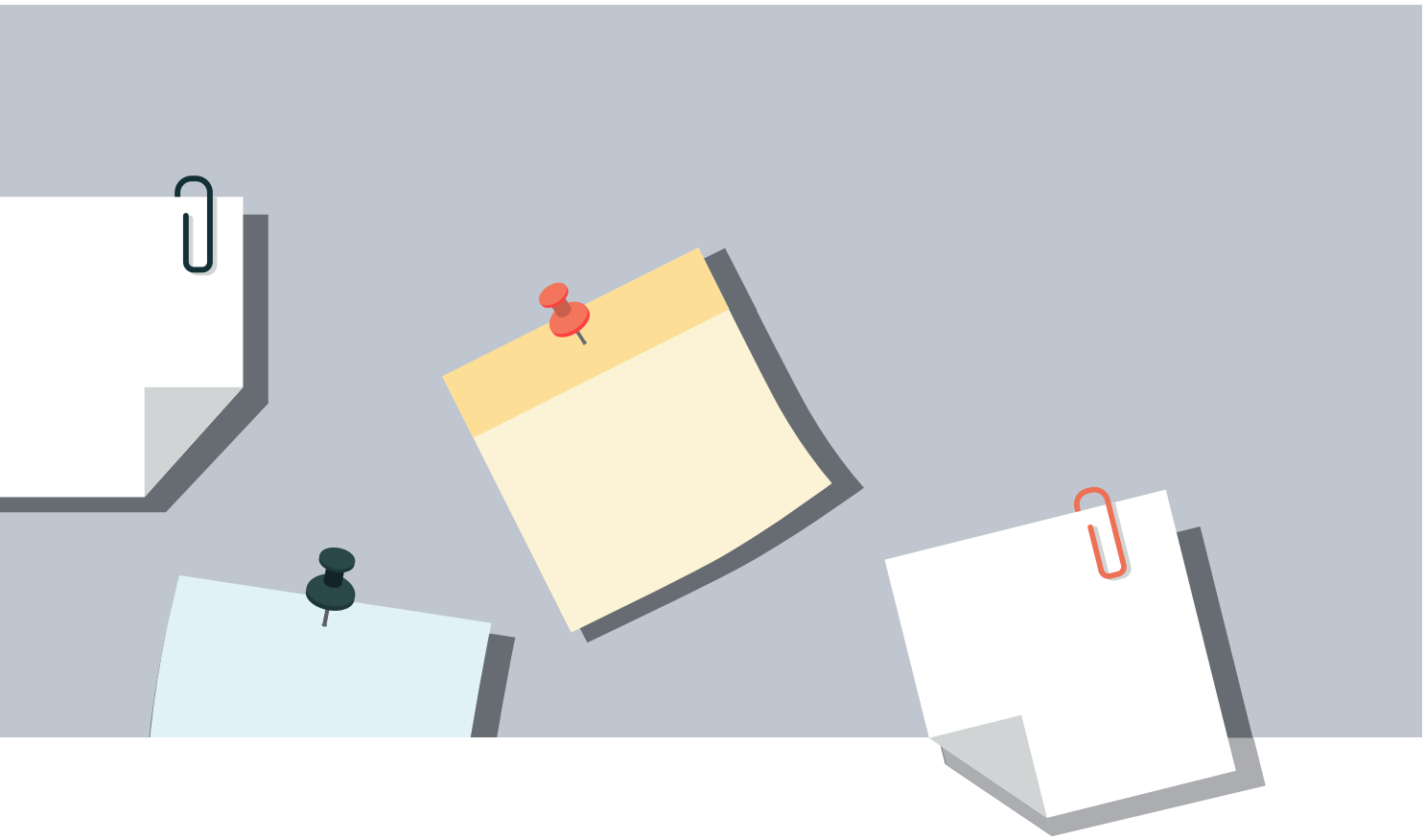
In September the UK Government announced plans for rolling out a free digital ID scheme in the UK for all UK citizens and legal residents.

The intention, as stated at the time, is for digital ID to be mandatory for proving right to work in the UK by the end of this parliament. Although another benefit heavily emphasised by Minister Josh Simons during the parliamentary debate on digital ID could be to radically simplify and improve people's access to public services. This benefit would be realised by providing a convenient single access portal, improving data security by preventing numerous individual parties from needing to gather and store personal data, and providing a mechanism for citizens' greater control and oversight of when their data is accessed and how it is used.

The UK government is not alone in its drive to build a digital ID system. Countries with established digital identification infrastructure include Estonia, Denmark, Finland, India, Singapore, Spain, and South Korea. Other countries are in the process of developing their own, including Canada and Germany.

However, the development and implementation of a government digital identity system is not without risk. The government is proposing to build from the ground up a foundational piece of digital public infratructure that will mediate how individuals' data is collected and shared and that will serve as a universal gateway to critical services. As such, there is ample opportunity to do significant harm. For example, a digital identification scheme developed and managed with inadequate attention to risks and safeguards could introduce new barriers to accessing critical public services for vulnerable populations. It could also provide the state with unprecedented access to personal data, enabling large-scale infringement on privacy rights with knock-on implications for other human rights such as rights to nondiscrimination, freedom of expression, movement and asylum.

A key challenge in the ongoing debate around digital ID is, however, that public details on the government's proposal for a digital identity scheme in the UK are currently lacking. A consultation is forthcoming in which further specific open questions will be shared, but in the meantime, the vagaries and information void surrounding the government's proposal have seeded speculation and misinformation, driving an increasingly polarised debate. At the time of writing a public petition opposing the scheme has reached nearly 3m signatures.



THE WORKSHOP

On December 8, 2025, **Demos** in partnership with the **Tony Blair Institute for Global Change (TBI)** coordinated and moderated a half-day workshop on the future of digital identification in the UK. The workshop agenda was developed in collaboration with the digital ID teams within the Department for Science, Innovation and Technology (DSIT) and the Cabinet Office (CO), and it was generously hosted by the Data Science Institute at the London School of Economics and Political Science (LSE), with DSIT and Cabinet Office attendance.

Hosted in the run up to DSIT's forthcoming consultation, the workshop brought together expert voices on digital ID and digital public infrastructure from across UK civil society, academia, and other stakeholder groups to consider the key challenges and opportunities for a digital identification program in the UK.

The day began with representatives from DSIT and the Cabinet Office presenting an update on current, in-process thinking about the form and function of the government's digital ID proposal. Participants then worked together reflecting on the DSIT/CO update to identify key challenges and clarifications the consultation will need to address.

This short briefing document summarises key points and findings from the day.

FRAMEWORK FOR **DEFINING DIGITAL ID**

The government needs to clearly define its digital ID proposal for the public in order to enable a productive consultation elucidating the risks and benefits specific to the proposal at hand.

Accordingly, the workshop's first challenge was to consider how digital identification should be defined. Our goal was not to stipulate the specifics of a comprehensively defined digital ID scheme - indeed the consultation is fully in service of this endeavour - but to offer a framework for what features ought to be included.

We identified four categories of digital ID scheme features that should be included and refined as part of a comprehensive definition for digital ID. Each is briefly described below.

TABLE 1
COMPONENTS OF A COMPREHENSIVE DEFINITION FOR A DIGITAL IDENTIFICATION PROGRAMME

DIGITAL IDENTIFICATION			
Needs, purpose, use cases	**Technical features**	**Governance details**	**Supporting programmes**
The social/public needs the scheme is meant to service, and the intended applications that will enable delivery of these benefits.	The hardware, software, data, and design features that underpin the basic functionality of the digital identification system.	How and by whom will the digital identification programme be delivered, managed, overseen, regulated, and financially maintained.	The additional external support and initiatives needed to successfully deliver a digital identity programme (e.g., additional support for digital inclusion, cybersecurity, digital literacy etc.)

1. NEEDS, PURPOSE, USE CASES

The form of the UK's digital ID scheme must be built around its intended function. The intended purpose and use-cases of digital ID will determine the technical features with which the system needs to be endowed, as well as the surrounding governance and support structures needed to maintain the scheme's efficacy and safety.

So far, the government has focused on immigration control and simplified public service delivery as two potential benefits at the top of public mind, but these assumptions should be confirmed and further refined into specific use-cases (e.g. right to work checks, voter registration, paying council tax, transferring health records etc.) via public consultation and deliberation.

Public buy-in to the digital ID scheme and its intended purposes will be critical to its success - both as a transformative bit of infrastructure happily adopted and as a political win. However, identifying public needs and specifying desirable and acceptable use cases based thereon (or unacceptable red-lines) is far from simple, nor is it a one-and-done exercise. Even within our technically very well informed group, disagreements were clear. The use of any form of digital ID as a gate to voter registration, for example, was a clear point of contention.

2. TECHNICAL FEATURES

Once purpose and function are determined, then the necessary technical features and safeguards of a digital identification system can be clarified. Technical features pertain to the hardware, software, data, and design that underpin the basic functionality of a digital identification service. Technical features include, for example, where data is stored, how data is shared or firewalled, and how user interfaces are designed to facilitate or encourage different functionalities.

These technical features of a digital ID system draw hard lines around what the system is and is not able to do and therefore also place initial technical constraints on how the system and its infrastructure could potentially be used or misused by current or future controllers. At the same time, one of the challenges of successful delivery is to ensure that technical decisions made at this stage do not lock the scheme into a form that cannot be readily iterated and adapted as technical capabilities, threats and understanding of benefits evolve.

Key questions on technical features raised during the workshop include:

- **Identity attributes** - What personal attributes should constitute (add up to) a digital identity?
- **Data storage** - Where should personal data be stored? (e.g., directly on the device, or in an external database). And should that storage differ for different kinds of data? (e.g., government might centrally store names, birthdays, and passport numbers, but maybe high resolution biometric pictures stay on devices)
- **Dataset centralisation** - Are databases centralised or federated? What firewalls exist between data sets? Are new datasets likely to be created or will only existing data be used?
- **Digital devices** - Can digital identification only be accessed and shown on smartphones?
- Data sharing - If databases are federated, how can seamless data sharing still be facilitated (if it should be facilitated) to realise the efficiency benefits for users?
- **User Experience (UX) design** - How is UX Design being implemented and does it take into account the needs of different user groups, such as identity holders or those carrying out checks? (e.g., what features will best allow people greater control over their data?)

- **Data minimisation** - What technical safeguards can help ensure data minimisation (that authorities requesting identity checks are only able access the minimum data needed for their purposes)
- **State interaction** - How will different parts of the state with existing digital ID infrastructure and datasets interact? (e.g. One Login and e-visas)

3. GOVERNANCE DETAILS

A digital identification scheme is much more than the technical infrastructure that gives it form. The efficacy, safety, impact of digital ID implementation will be heavily influenced by its initial and ongoing governance.

Digital ID programme governance refers to the definitions, rules, policies, processes, and legal frameworks directing or enabling continued use and maintenance of digital ID systems - for example rules pertaining to when people are allowed to be asked to show ID, about if and how digital ID data can be accessed or used by law enforcement, about who is licensed to provide digital ID and verification services, and more generally, about who has authority to make these decisions and by what mechanism.

Key considerations about digital ID governance raised in our workshop pertained to (a-b) what governance structures and processes will exist around the UK's digital ID scheme and (c) specific rules and requirements around digital ID implementation and use that need clarification.

(a) Governance structure

- **Operation** - Is this a fully public, government owned and operated endeavour or is there space for private digital ID service providers?
- **Oversight** - Where would independent oversight of a government digital ID programme sit? What powers should that body have? How should it be future-proofed?
- **Funding** - Government budgets shift. What plans will be put in place to ensure that the digital ID scheme (the system itself and surrounding supports) will be adequately funded in the long term to be maintained as fit-for-purpose public infrastructure?

(b) Governance process

- **Regulation** - Will the digital ID scheme be accompanied by regulation (e.g., on acceptable use cases, data protection requirements, etc.) that will be brought forward for parliamentary scrutiny and vote?
- **Transparency** - How will ongoing developments regarding the digital ID scheme and, once the roll-out begins, its performance (e.g., error/fraud rate) be communicated to the public?
- **Consultation** - At what stages of policy development should public input be engaged, and by what mechanisms? Workshop participants noted that long-form written consultations are not always the best for elucidating public needs and values and that government might also look to engage in public deliberation processes, possibly mediated by AI tools that enable scaled deliberation at low cost.

(c) Rules, requirements, and restrictions

There are numerous open questions regarding the rules, requirements, and restrictions that will surround the UK's digital ID system – both facilitating and confining its functionality and use. These will be established, enforced, and, over time, revised, within the governance structures and processes determined above.

The following list is by no means exhaustive, but presents a set of key questions raised during the workshop about the parameters of the government's digital ID proposals that are significant sources of concern as well as unproductive speculation. These are priority targets for clarification.

- **Use cases** - In what situations can citizens be asked to present their digital credentials? Will there be any red-line cases (e.g., for accessing emergency healthcare) when citizens should never be asked, and how would these be established and maintained (e.g., legislatively)?
- **Data minimisation** - Will data minimisation principles be implemented? If so, how much data needs to be presented to different actors to satisfy minimum verification needs? How will minimum data exposure requirements be determined and technically enabled?
- **Data access and consent** - When are government actors authorised to view and process citizen data? Will/how will citizens be able to give consent for data access and processing? What technical constraints will limit potential government abuse of citizen data access in future? What forms of consent would be considered appropriate, given that there are almost always some forms of interaction with government that are not based on consent?
- **Mandatory or voluntary** - Will it be a mandatory requirement for everyone to hold a digital identification? The government's current position is that it won't be mandatory - but what guarantees might there be in the future? Will it be mandatory for some specific activities (e.g., right to work checks)? There is currently residual ambiguity.
- **Age of qualification/requirement** - At what age will people qualify for or be required to register for a digital ID? It is a balance between preventing children from accessing associated benefits, protecting children from data privacy risks, and dealing with the complication that children don't carry smartphones as well as wider questions about the age of consent.
- **Area of operation** - Where will digital ID be implemented? UK wide or England? Will it be interoperable in some form with similar initiatives in the EU?
- **Redress & remedy** - What avenues will be available for people to request corrections to their data and to voice grievances and seek redress for suspected harms stemming from system errors or mismanagement? How can those requests be addressed quickly without creating another source of backlogs and bottlenecks in government?

The broader concerns stemming from these questions and others explored in this section are summarised in the following section.

4. SUPPORTING PROGRAMMES

Finally, a digital identification scheme will require external support to enable effective maintenance and administration and to ensure users are empowered to benefit from the new systems. There is no path forward for digital ID in the UK if, for example, it is based solely on a smartphone app but people do not have reliable access to personal smartphones on which the digital credential can be displayed. A large scale and ongoing digital inclusion program will therefore need to be implemented as an essential support for the UK's digital ID scheme. Critical support programs such as a digital inclusion programme should be considered constituent to a comprehensive definition for digital ID, and clear plans for their delivery and maintenance ought to be articulated accordingly.

Key support programs considered during the workshop include:

- **Digital inclusion** - a programme aimed at either ensuring everyone who wishes to use digital devices has access to the devices needed to utilise digital ID and other digitally mediated services; or that those who are digital excluded are otherwise able to access the benefits of digital ID.
- **Digital literacy & use support** - a programme aimed at ensuring all citizens who wish to use digital ID have (a) convenient access to support for learning how to use their digital devices and the digital ID interface, and (b) a known and easily accessed point of contact for ongoing support if/and when additional help is needed (e.g., with setting up your digital ID on a new phone).
- **Policy and rights awareness education** - a programme aimed at ensuring citizens understand what digital ID is and how it explicitly can and cannot be used by the state, and that citizens understand their rights and protections with respect to digital ID use (e.g., when people are allowed to ask for ID) and how to seek redress in case of error or suspected rights infringement.
- **Cybersecurity initiatives** - a programme aimed at supporting robust cybersecurity protection around digital ID infrastructure and data sets which will likely become major targets for attack.
- **Associated funding** - notably, a number of these support services are currently provided in large part by non-profit and charity organisations. These organisations might still be leveraged as a mechanism (or part of a mechanism) for support service delivery, but the government should be aware that the introduction of a digital identification scheme would substantially increase demand on these organisations at significant financial cost. Whether the government is delivering the support programmes independently or through existing organisations, the government will still need to plan for associated funding to cover the increased financial burden.

SUMMARY OF **KEY CONCERNS**

During the workshop participants compiled a list of chief concerns - the possible pitfalls of an improperly set-up and inadequately safeguarded digital ID systems, or alternatively the trade-offs that might have to be navigated. Some will view these concerns as a list of arguments against a UK digital ID scheme. Another perspective is to look at them as a list of system requirements that must be carefully addressed in further policy development and by ongoing governance activities to deliver a safe and beneficial form of digital identification infrastructure for the UK public.

1. DATA PRIVACY AND SECURITY

A national digital ID scheme could, depending on design choices, enable mass, centralised data collection. How do we ensure only essential data is held and accessed? If identity datasets are centralised, this could create an enormous hacking target potentially raising the risk of catastrophic identity theft events or incidents that would compromise privacy and undermine public confidence in the programme. Some design choices could also lead to providing central government with unprecedented access to comprehensive data on all citizens, which could be leveraged for nefarious purposes.

- Where will data associated with digital identities be stored?
- Will it be centralised or siloed?
- What restrictions will be placed around data linking?
- Is it possible for some data (e.g., high resolution photos) to be stored directly on the devices?

Note: *During the parliamentary debate on digital identity on December 8th (subsequent to this workshop), Minister Simons clarified that the UK would not be creating a centralised master database. It will be a federated database with strict legal firewall restricting what information can be shared and with strong principles of consent and data minimisation.*

2. RISKS OF (DE)CENTRALISED OWNERSHIP AND CONTROL

Centralised ownership and control of the national digital identity system by the government facilitates the convenience of joined up functionality and establishes digital ID as public infrastructure maintained for public good. However, a fully government owned and operated system could undercut the private digital identification verification industry which has well established standards of operation and brings billions of pounds to the UK economy. Furthermore, it means one entity has control over a massive critical infrastructure which conveys substantial power to that entity and introduces a single point of system failure in case of system mismanagement.

In the case the national digital identification system is constructed so as to integrate a diversity of private digital identity verification providers, the single-failure point risk is mitigated and the private industry set to thrive. However, new challenges emerge regarding system efficiency and convenience for users, how to effectively integrate the range of platforms with different government services to deliver the intended benefits, and how to manage mass data sharing between government and the private providers.

- How will the private identification verification industry be impacted in case of a central publicly owned and operated digital identification system?
- Is there a place for private contractors in a public identification system?
- For a centralised system, how could single-point infrastructure failure vulnerabilities be mitigated? (e.g., through funding plans, governance structures, or system redundancies?)

> ***Note:*** *Minister Simons's speech stated that the digital identification system will be publicly owned, operated, and governed.*

3. SCOPE CREEP AND HUMAN RIGHTS INFRINGEMENTS

Once a digital identification system exists, its use and application space might be expanded to enable broader surveillance, profiling, and tracking functions, even if these functionalities were initially deemed unacceptable. The implications for human rights – notably rights to privacy and to freedoms of expression, assembly, and movement – could be significant. Pervasive identification requirements and active monitoring can create a chilling effect, discouraging people (primarily minority and marginalised communities) from seeking and sharing information, socialising, participating in protests, or moving freely.

More so, scope creep may not be obvious. It could, under some circumstances, occur slowly through small, incremental changes to policy for seemingly justified reasons. These small changes might not raise alarm in isolation but could amount to an unacceptable development in digital identification functionality and use. Even if the current government is serious about pursuing only pro-social goals with its digital identification scheme, the risk of the platform being utilised by less democratically-minded administrations down the line must be considered.

- What strict red-lines around digital identification use-cases will be drawn in regulation to mitigate risk of scope creep?
- Will red-lines be drawn around digital identification requirements and use cases that threaten human rights?
- What technical features will be built into the system to constrain undesirable applications and rights infringements?
- Would it be possible to establish as a standard the national digital identification system that it only improves conditions for underserved and minority populations from the status quo?

4. DIGITAL EXCLUSION

If digital ID is an essential gateway to digital services, people who don't have smartphones, internet access, or adequate digital literacy may be inadvertently barred from access. These consequences are likely to be felt primarily by communities that are already underserved.

- Will digital identification be mandatory for all citizens and legal residents, or will there be specific services or scenarios for which digital identity will be mandatory?
- What alternative forms of identity will be accepted?
- Will public services be as easy to access with digital identification as with alternative forms?
- How will people be supported in acquiring digital devices and learning to utilise the digital identification interface on an ongoing basis?

> ***Note:*** *Minister Simons's speech confirmed that the digital identification scheme would be accompanied by a large-scale digital inclusion programme.*

5. IDENTITY EXCLUSION

Identify exclusion is when people are unable to have their identities accurately recognised – for example when physical IDs do not match a person's current presentation – which can lead to marginalisation and denied access to services, opportunities, and full social participation. Identity exclusion disproportionately affects minorities, disabled people, migrants, and youth, and can have significant economic, social, and psychological costs. While identity exclusion is not a new challenge presented by a digital identification scheme, the establishment of a new national digital identity system will require grappling directly with questions about how identities (and which identities) are represented and acknowledged. Key concerns pertain to the representation of race and gender diversity.

- What personal attributes will be used to comprise a digital identity?
- How will the full diversity of those attributes be represented?

6. FRAUD

A national digital identity system will have to counter fraud risks stemming, for example, from identity theft, account takeover, and the creation of synthetic or duplicate identities that can be used to access services or benefits illegally. On the other hand, if it is robustly designed, a digital identity system could also significantly reduce fraud by providing stronger, more consistent verification of individuals across services, making it harder to forge documents or assume false identities.

- What technical features will be built into digital identification systems to prevent fraud (e.g., multi-factor authentication, data sharing protocols, etc.)
- Will the government publish fraud data to demonstrate the efficacy of the digital identification system in this respect?
- Will new vectors of fraud be created by a digital ID system, such as offering vulnerable people help in setting it up for an additional charge?

7. REDRESS AND REMEDY

No digital identity system will be perfect. There will be occasional errors (e.g., mistakes in data records or instances of unauthorised data sharing) and individuals may suffer harm as a result – perhaps they are unjustly denied access to services or not allowed to work or to travel. In these instances, mechanisms for redress and remedy are needed. People must be able to raise complaints, see errors fixed quickly, and receive compensation or reparation for any harms caused.

During the workshop, participants noted the substantial administrative support that an adequate reporting, redress and remedy mechanism would require. The process of noting an error in a data record, putting forward a change, and having that change verified and implemented may involve numerous people and services. Nonetheless, to ensure that people have adequate control over their data and to help maintain a fair and just digital identification system, mechanisms for reporting and redress will need to be smooth, accessible, and easily navigated by all.

- What human administrative support will be in place to facilitate error reporting, redress, and remedy processes?
- Will sufficient resources be provided to prevent the emergence of new backlogs or bottlenecks around these processes?
- Will the government publish error reporting and remedy data (distinct from fraud data) to evidence responsiveness?

8. RESILIENCE TO TECHNOLOGICAL CHANGE

Concerns were raised during the workshop about whether the national digital identity proposal would be sufficiently resilient to technological change. By relying heavily on smartphones as the primary means of authentication, the system could quickly become outdated if user devices or prevailing digital practices shift significantly. Emerging technologies - such as new biometric methods, decentralised identity models, or alternative hardware - may require substantial redesigns that undermine the value of the initial investment.

- How will flexibility be built into the digital ID system, its ongoing delivery and governance, to ensure long term adaptability?

9. DELIVERABILITY

Building and securely maintaining the complex technical, legal, and administrative infrastructure required to deliver a well-functing digital identification scheme as imagined by the government is an immense undertaking. However, the ambition to deliver it before the end of this Parliament means that the government only has three years. As this brief has illustrated, there are numerous considerations that must be taken into account to mitigate any potential harms and to deliver on the benefits promised. More so, the switch to digital ID would be a significant transition for the public, requiring new digital devices, new skills, and a shift away from familiar processes.

- Is three years a feasible time-frame for delivering a fully fledged and functional digital ID scheme for the UK?
- Can government share a timeline for the digital ID development and rollout plan? This might include timings on policy consultation, development and parliamentary consideration of any company legislation, digital inclusion program rollout, digital ID system design and testing, building administrative capacity, implementation stages.

10. COST

The national digital identity system will be free at the point of use, but would still carry costs for government to develop, maintain, and support, and these costs would ultimately be borne by UK taxpayers. The proposal also risks deepening reliance on charities that already shoulder much of the burden for providing essential support services, like digital inclusion programs and digital skills training. These organisations may face heightened pressure and escalating costs with the wide-rollout of digital ID that will also need to be met with government funds to ensure the programme's success.

If digital identity is to become foundational national infrastructure, a plan for sustainable funding of the full scheme (the technology, its administration, maintenance and support) will be needed. Government budgets change, any future funding withdrawal could have substantial consequences, undercutting the benefits and causing harm.

- What are the projected costs of establishing and maintaining the digital identification scheme? This should include costs associated with its ongoing administration and of delivering (or supporting third parties to deliver) critical support programs such as digital inclusion initiatives, skills development, and accessible support services.

AN OPPORTUNITY FOR **BUILDING TRUST**

The government has made a large political bet in championing its plan for digital identification in the UK, and pursuing despite some clear public opposition. It is a large-scale programme and did not feature as a Manifesto promise. While there are differences in the schemes, the previous attempt by the last Labour government to deliver an identity scheme was scrapped in 2010 by the Conservative government for being "intrusive, ineffective and enormously expensive".

When the present digital identity scheme was announced, it came on the scene suddenly, it was framed as a crackdown on immigration with only buried mention of wider benefits, and it was met with very vocal opposition.

With government approval ratings in decline, the government would need to deliver a resoundingly successful digital ID program with tangible benefits. In particular, it would need to directly address current frustrations with government and realise tangible improvement to public service delivery that people will feel.

But it's not just about the end product. The announcement was unexpected and public concerns about privacy, security, and impacts on human rights are justified in the absence of greater detail, seeding understandable scepticism and doubt. The government should fully harness the opportunity consultation provides to help bring the public into the discussion, to demonstrate a willingness to listen and to respond in accordance with what's heard. In doing so, it also has an opportunity to model a new form of engagement with experts and the public, including, as one participant observed, through the use of new technologies like AI-assisted engagement tools to carry out a genuinely wide-ranging study of views and attitudes.

Digital identification is not just an opportunity to realise efficiencies and streamline service delivery. The broader debate that it has sparked is an opportunity to engage people in two-way dialogue and to start repairing trust if handled well. Either to mishandle the consultation process or to deliver a product that is subpar could be catastrophic for public trust in government at this vulnerable time.

Note: *Minister Simons's speech confirmed his intention to go beyond traditional consultation to "travel up and down the country to listen to people and hear how they want this credential to work".*

TELLING **THE STORY**

Finally, at the end of the workshop participants discussed the overarching need for the government to improve the narrative around the digital identification scheme, the plan and its purpose. One participant commented that they'd just sat through a four hour workshop learning and debating the ins and outs of digital identity, and that our room was now probably one of better informed groups of people on the topic in the country. Yet they still didn't really understand why the government is pushing for a digital identification scheme. Why now, and why should they be excited about it? And if the grand story hadn't clicked for everyone in our group yet, we certainly shouldn't expect the public to be convinced.

The government's story on the 'why' of digital identity has shifted a couple times. In the first case they did not focus on public benefits, instead tapping into a polarising debate around immigration. Immigration is absolutely a topic that will need to be grappled with (regarding how digital identification can, should, or should not be leveraged to influence immigration or monitor immigrants) but it is by no means the whole picture, nor the factor that will matter most or deliver real change for most people.

The group expressed a desire to see and understand the real, deeper narrative about public value. **There needs to be a genuine story about the relationship between citizens and state, the state's obligation to listen and serve inline with public needs and value, and about how a digital identification program will be developed and implemented to this end.**

Licence to publish

Demos – Licence to Publish

The work (as defined below) is provided under the terms of this licence ('licence'). The work is protected by copyright and/or other applicable law. Any use of the work other than as authorized under this licence is prohibited. By exercising any rights to the work provided here, you accept and agree to be bound by the terms of this licence. Demos grants you the rights contained here in consideration of your acceptance of such terms and conditions.

1 Definitions

a 'Collective Work' means a work, such as a periodical issue, anthology or encyclopedia, in which the Work in its entirety in unmodified form, along with a number of other contributions, constituting separate and independent works in themselves, are assembled into a collective whole. A work that constitutes a Collective Work will not be considered a Derivative Work (as defined below) for the purposes of this Licence.

b 'Derivative Work' means a work based upon the Work or upon the Work and other pre-existing works, such as a musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which the Work may be recast, transformed, or adapted, except that a work that constitutes a Collective Work or a translation from English into another language will not be considered a Derivative Work for the purpose of this Licence.

c 'Licensor' means the individual or entity that offers the Work under the terms of this Licence.

d 'Original Author' means the individual or entity who created the Work.

e 'Work' means the copyrightable work of authorship offered under the terms of this Licence.

f 'You' means an individual or entity exercising rights under this Licence who has not previously violated the terms of this Licence with respect to the Work, or who has received express permission from Demos to exercise rights under this Licence despite a previous violation.

2 Fair Use Rights

Nothing in this licence is intended to reduce, limit, or restrict any rights arising from fair use, first sale or other limitations on the exclusive rights of the copyright owner under copyright law or other applicable laws.

3 Licence Grant

Subject to the terms and conditions of this Licence, Licensor hereby grants You a worldwide, royalty-free, non-exclusive, perpetual (for the duration of the applicable copyright) licence to exercise the rights in the Work as stated below:

a to reproduce the Work, to incorporate the Work into one or more Collective Works, and to reproduce the Work as incorporated in the Collective Works;

b to distribute copies or phono-records of, display publicly, perform publicly, and perform publicly by means of a digital audio transmission the Work including as incorporated in Collective Works; The above rights may be exercised in all media and formats whether now known or hereafter devised. The above rights include the right to make such modifications as are technically necessary to exercise the rights in other media and formats. All rights not expressly granted by Licensor are hereby reserved.

4 Restrictions

The licence granted in Section 3 above is expressly made subject to and limited by the following restrictions:

a You may distribute, publicly display, publicly perform, or publicly digitally perform the Work only under the terms of this Licence, and You must include a copy of, or the Uniform Resource Identifier for, this Licence with every copy or phono-record of the Work You distribute, publicly display, publicly perform, or publicly digitally perform. You may not offer or impose any terms on the Work that alter or restrict the terms of this Licence or the recipients' exercise of the rights granted hereunder. You may not sublicence the Work. You must keep intact all notices that refer to this Licence and to the disclaimer of warranties. You may not distribute, publicly display, publicly perform, or publicly digitally perform the Work with any technological measures that control access or use of the Work in a manner inconsistent with the terms of this Licence Agreement. The above applies to the Work as incorporated in a Collective Work, but this does not require the Collective Work apart from the Work itself to be made subject to the terms of this Licence. If You create a Collective Work, upon notice from any Licensor You must, to the extent practicable, remove from the Collective Work any reference to such Licensor or the Original Author, as requested.

b You may not exercise any of the rights granted to You in Section 3 above in any manner that is primarily intended

for or directed toward commercial advantage or private monetary compensation. The exchange of the Work for other copyrighted works by means of digital file sharing or otherwise shall not be considered to be intended for or directed toward commercial advantage or private monetary compensation, provided there is no payment of any monetary compensation in connection with the exchange of copyrighted works.

c If you distribute, publicly display, publicly perform, or publicly digitally perform the Work or any Collective Works, you must keep intact all copyright notices for the Work and give the Original Author credit reasonable to the medium or means You are utilizing by conveying the name (or pseudonym if applicable) of the Original Author if supplied; the title of the Work if supplied. Such credit may be implemented in any reasonable manner; provided, however, that in the case of a Collective Work, at a minimum such credit will appear where any other comparable authorship credit appears and in a manner at least as prominent as such other comparable authorship credit.

5 Representations, Warranties and Disclaimer

a By offering the Work for public release under this Licence, Licensor represents and warrants that, to the best of Licensor's knowledge after reasonable inquiry:

i Licensor has secured all rights in the Work necessary to grant the licence rights hereunder and to permit the lawful exercise of the rights granted hereunder without You having any obligation to pay any royalties, compulsory licence fees, residuals or any other payments;

ii The Work does not infringe the copyright, trademark, publicity rights, common law rights or any other right of any third party or constitute defamation, invasion of privacy or other tortious injury to any third party.

b Except as expressly stated in this licence or otherwise agreed in writing or required by applicable law, the work is licenced on an 'as is' basis, without warranties of any kind, either express or implied including, without limitation, any warranties regarding the contents or accuracy of the work.

6 Limitation on Liability

Except to the extent required by applicable law, and except for damages arising from liability to a third party resulting from breach of the warranties in section 5, in no event will licensor be liable to you on any legal theory for any special, incidental, consequential, punitive or exemplary damages arising out of this licence or the use of the work, even if licensor has been advised of the possibility of such damages.

7 Termination

a This Licence and the rights granted hereunder will terminate automatically upon any breach by You of the terms of this Licence. Individuals or entities who have received Collective Works from You under this Licence, however, will not have their licences terminated provided such individuals or entities remain in full compliance with those licences. Sections 1, 2, 5, 6, 7, and 8 will survive any termination of this Licence.

b Subject to the above terms and conditions, the licence granted here is perpetual (for the duration of the applicable copyright in the Work). Notwithstanding the above, Licensor reserves the right to release the Work under different licence terms or to stop distributing the Work at any time; provided, however that any such election will not serve to withdraw this Licence (or any other licence that has been, or is required to be, granted under the terms of this Licence), and this Licence will continue in full force and effect unless terminated as stated above.

8 Miscellaneous

a Each time You distribute or publicly digitally perform the Work or a Collective Work, Demos offers to the recipient a licence to the Work on the same terms and conditions as the licence granted to You under this Licence.

b If any provision of this Licence is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Licence, and without further action by the parties to this agreement, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable.

c No term or provision of this Licence shall be deemed waived and no breach consented to unless such waiver or consent shall be in writing and signed by the party to be charged with such waiver or consent.

d This Licence constitutes the entire agreement between the parties with respect to the Work licenced here. There are no understandings, agreements or representations with respect to the Work not specified here. Licensor shall not be bound by any additional provisions that may appear in any communication from You. This Licence may not be modified without the mutual written agreement of Demos and You.

DEMOS

PUBLISHED BY DEMOS JANUARY 2026

15 WHITEHALL, LONDON, SW1A 2DD
T: 020 3878 3955
HELLO@DEMOS.CO.UK
WWW.DEMOS.CO.UK