Which?
2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

c/o Digital ID
Cabinet Office
70 Whitehall
SW1A 2AS

Consultation Response

Which? response to the Cabinet Office's consultation on Making public services work for you with your digital identity

Submission date: 05/05/2026

Summary

Which? welcomes this opportunity to respond to the Cabinet Office consultation on 'Making public services work for you with your digital identity'.[1] The government is proposing an optional digital ID (the national digital ID) that will be a government-owned product in the form of a credential that can be held in the GOV.UK digital wallet covering attributes of name, date of birth, nationality and a biometric facial image. The consultation sets out that the government primarily intends the national digital ID to streamline citizens' access to public services and support digital right to work checks. However, the government also suggests that the national digital ID could end up being used in consumer use cases (such as verification of age for age-restricted purchases like alcohol); so we believe it is important that the government considers outcomes for consumers and we find the lack of consumer recognition in the consultation concerning.

Our response specifically focuses on consumers and consumer use cases rather than citizens or the wider public. A summary of the key points we make in our response follows.

Consistent high standards across the entire market:
We agree that a national digital ID has the potential to offer benefits for consumers. This could be through more streamlined, frictionless services when attribute or identity verification is required in consumer use cases, such as verifying age for alcohol purchasing. It can also reduce the risks of loss or damage to important physical ID documents, as well as give consumers more control over their data through adherence to the principles of data minimisation and selective disclosure.

It is vital that the national digital ID is held to at least the same standards as private providers accredited against the UK digital verification services trust framework (DVSTF). This will prevent the creation of a two-tier system where consumers may have different

[1] Cabinet Office (2026), *Making public services work for you with your digital identity* . Available at: https://www.gov.uk/government/consultations/making-public-services-work-for-you-with-your-digital-identity

experiences using the national digital ID versus using certified private providers, yet currently DVSTF accreditation is not required of the national digital ID.

Digital inclusion for consumers, and consumers' experiences of creating and using the national digital ID:
We support the plan for alternative access routes (provided they are sufficiently secure), but also wish to highlight that digital exclusion in relation to the national digital ID can play out in two ways: it may be difficult to get and use the digital ID, or it may be difficult to access other services that rely on digital ID.

Processes for creating, updating and deleting the national digital ID must be user-friendly and straightforward for consumers, and the onboarding process must be secure to prevent infiltration by fraudsters.

We believe the proposal for a legal requirement for national digital ID users to inform the government of changes in their attributes is too onerous for consumer use cases. We believe that for consumer use cases, users should only have a duty to ensure their attributes are up to date at the point of use.

It is important that the government considers and monitors consumer outcomes and use cases as it develops the national digital ID. This may help inform decisions about digital inclusion and redress, while also aiding considerations about which attributes to include and the processes for creating, updating and deleting the national digital ID.

Full response

Part 1: Our Ambition

Which? agrees that consumers can benefit from digital ID. Digital ID has the potential to help streamline identity verification in consumer journeys, reduce the risks of loss or damage to important physical ID documents, and give consumers more control of their own data and how much they share.[2]

It is also worth acknowledging that many consumers are already using forms of digital ID technology. For example, consumers are accustomed to using biometric technologies like voice, fingerprint or facial recognition for actions like phone banking security checks, unlocking digital devices like smartphones, using digital wallets[3], or authenticating online payments. These uses of biometric identity information do not require certification against the government's digital verification services trust framework (DVSTF) as they are not accessing government-held information.

---

[2] TechUK (2024) *How DSIT is enabling the use of trustworthy digital identity services in the UK.* Available at: https://www.techuk.org/resource/how-dsit-is-enabling-the-use-of-trustworthy-digital-identity-services-in-the-uk.html

[3] A digital wallet is a software application that can digitally store information, including credit/debit cards, tickets and loyalty cards, and support secure contactless payments with a smartphone.

We support the work to date within the Department for Science, Innovation and Technology (DSIT) to develop the DVS Trust Framework (DVSTF) which sets the rules and standards that private digital verification services (DVS) providers must meet. We believe that the national digital ID proposed in this consultation can add to consumer choice of DVS providers, but it is critical that the national digital ID adheres to at least the same standards as private providers certified against the DVSTF. Currently there is no clear proposal for the national digital ID to be officially certified against the DVSTF.

If the national digital ID is not required to be certified against the DVSTF, there are potential risks of creating a two-tier system where consumers may have different experiences (due to inconsistent standards) using the national digital ID versus using certified private providers. Inconsistencies across the market may leave consumers exposed to inferior experiences or outcomes, affecting consumer trust in the market as a whole. We note that GOV.UK lost its DVSTF accreditation last year[4] and the government has not yet stated that the proposed national digital ID will be required to formally gain accreditation.

Part 2: Our approach

Chapter 2.1: Creating the digital ID

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

The government must ensure that the national digital ID is held to the same standards as private providers as set out in the DVSTF.

Chapter 2.2: Storing, managing and using the digital ID

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

It is important that consumers have the ability to delete their national digital ID if they no longer want it. We support the consultation's proposal that this process will be simple and quick. We would encourage user testing of this process to ensure it is a straightforward process for consumers.

We note that this chapter states that attributes in the digital ID will need to be alterable in case of errors in the issuance process. However, there is no mention of fixing errors (as opposed to deletion) in the questions in this chapter. Question 3 in Chapter 3.1 is the only consultation question that mentions errors, but this focuses on resolving 'errors' that arise from intentional changes the consumer has made (such as name changes). There are no

[4] ComputerWeekly.com (2025) *Gov.uk One Login loses certification for digital identity trust framework*. Available at: https://www.computerweekly.com/news/366623835/Govuk-One-Login-loses-certification-for-digital-identity-trust-framework

questions addressing when the errors occur at the issuance of the digital ID and when they are due to things outside of the consumer's control. We think this is an oversight. It is important for the government to consider not only how consumers can delete their national digital ID, but also what the process will involve for consumers who need to resolve errors in their national digital ID. This should involve clear information about liability, redress mechanisms and where to go for help. We find the absence of proposals for consumer redress concerning. We would recommend that the government monitor consumer outcomes as usage of digital ID grows and revisit whether new or additional redress routes are required if consumers are experiencing harms that are specific or unique to the digital ID market.

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

We agree that revocation should only occur in strictly controlled circumstances and be governed by robust processes. The government must clarify what these processes will involve and how they will be developed and finalised.

We note that revocation is likely to be reserved for when identity fraud is detected. Signs of identity fraud could include accounts being opened in the victim's name that the victim does not recognise, or the victim receiving bills for accounts they do not recognise. Yet it is not clear how the government would be able to identify this before the victim does. Clarity is needed on whether the government intends to be able to revoke a digital ID unilaterally and what mitigations will be in place, as this approach could have unintended consequences in the event of false positives (including from automated anti-fraud checks). We would encourage the government to consider how it could communicate with consumers prior to revocation, particularly where revocation is due to the consumer being victimised. We anticipate that this system might work more effectively if the government revokes a digital ID following a report from the victim and also provides support for the victim to secure their identity.

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

We support consumers being able to choose to store their national digital ID in digital wallets offered by other providers in addition to the GOV.UK wallet, provided appropriate standards are met and maintained. One of the consumer benefits of digital ID is the ease-of-use benefits of not having to carry or purchase physical ID documents. To give these benefits the best chance of being fully realised by consumers, there need to be as few barriers as possible to accessing and using the national digital ID. Where it is stored could be a potential barrier.

There is some evidence that indicates consumers have a preference to use a single digital wallet that serves all their needs (including payments, tickets and digital ID). A McKinsey digital payments survey in 2023 found the share of people expecting to rely on a single wallet was increasing, with more consumers preferring a single wallet than using multiple

wallets for different purposes.[5] This is supported by findings from a survey of Which? members in April 2026, where around half (51%) of respondents said they used a digital wallet because “it’s convenient to have everything in one place”. When asked to indicate their preference between potential features of a digital wallet that could emerge in the future, the ability to store ID documents in their digital wallet was ranked highest by Which? members.[6]

There is also evidence that consumers have a preference for a smaller number of apps. A survey by Amplitude in 2025 found that “consumers are intentional about app management, with almost half (44%) of people saying they limit the number of apps they download to avoid phone clutter”.[7] This may be even stronger for people with older phones with more storage limitations, which could be more frequent among low-income consumers.

Friction when downloading a new app can also lead to high rates of abandonment, especially if it does not work as expected when downloaded. The Amplitude survey found that "More than a third (35%) of UK consumers will ditch an app within minutes if it doesn’t function properly" and 10% will abandon an app within seconds. This issue was cited as a key reason behind the failure of the UK's previous digital identity platform, GOV.UK Verify, which was determined to have missed all its performance targets and failed its users in 2019 by the Public Accounts Committee (PAC).[8] The PAC noted "people have often found Verify “clunky” to use and many have faced problems even signing up with it in the first place".[9] This suggests that allowing existing digital wallet apps already in popular use to hold the national digital ID could lead to more successful take up.

Such an approach would be compatible with the approach being developed in the EU, where member states have discretion to determine whether they provide the European Union Digital Identity (EUDI) Wallet either directly, via a private party acting on the member state’s behalf, or by officially recognising a private party’s app that complies with the technical standards set out in the eIDAS 2.0 Regulation.[10]

---

[5] McKinsey (2023) *Consumer digital payments: Already mainstream, increasingly embedded, still evolving.* Available at: https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/consumer-digital-payments-already-mainstream-increasingly-embedded-still-evolving

[6] 1,252 Which? members were surveyed in April 2026. The sample was not nationally representative and strongly skewed toward older male members (85% above the age of 65+ and 69% male). Members who used digital wallets were asked to select from a list of reasons for using a digital wallet. They were also presented with a list of 11 potential digital wallet features and asked to select the three features they thought were best - in addition to storing digital ID, the list of features included the ability for a digital wallet to act as a financial hub, automate loyalty point collection and give greater control over subscriptions/contracts.

[7] Amplitude (2025) *The Silent Brand Killer: Tech Frustration in the UK.* Available at: https://amplitude.com/blog/uk-tech-frustration-survey

[8] Public Accounts Committee (2019) *Government flagship digital identification system failing its users*. Available at: https://committees.parliament.uk/committee/127/public-accounts-committee/news/98272/government-flagship-digital-identification-system-failing-its-users/

[9] Public Accounts Committee publication & records. *Performance, costs and benefits.* Available at: https://publications.parliament.uk/pa/cm201719/cmselect/cmpubacc/1748/174806.htm#_idTextAnchor006

[10] Baker McKenzie (2026) *European Union: EUDI Wallet Harmonizes Identification and Age-Gating*. Available at: https://www.bakermckenzie.com/en/insight/publications/2026/03/european-union-eudi-wallet-harmonizes-identification-and-age-gating

4. **To what extent do you agree or disagree with the proposed government checker service being made available for use in the private and third sectors, at low or no cost?**

The consultation proposes that most identity or attribute checking in the wider economy will be done by intermediary DVS providers and that the government checker service will be a version of this used in public sector settings. We do not oppose the government checker service being made available for use in consumer use cases, provided the consumer experience is not negatively impacted by which underlying DVS provider is being used to do the checking. We would also emphasise that robust checking of digital IDs is important to protect consumers, so regardless of the provider of both the ID and the checker service, appropriate standards must be met. We understand this is the intended purpose of the DVSTF and reiterate that the national digital ID must be certified to at least the same standards.

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

We do not have a strong preference for how the government checker service will be used in consumer use cases. However, we would support a focus on interoperability between different DVS and checker services to support consumer choice across use cases. It is important that consistent high standards are maintained no matter which checker service is being used. We would encourage the government to consult with consumers about their preferences for consumer use cases.

Part 3: Useful

Chapter 3.1: Information contained in the digital ID

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

We note that some other countries have national digital IDs which include other attributes, such as national personal identity numbers, sex or gender, and place of birth, although some of these may be 'recommended' rather than 'required' attributes.[11] We support the efforts not to include unnecessary attributes as this approach better aligns with the principle of data minimisation.

Discussions about pensions dashboards often mention digital ID as an enabler. For example, the Pensions Dashboard Programme (PDP) requires an identity service to allow

[11] See for example Sweden's attribute specification for the Swedish eID Framework: https://docs.swedenconnect.se/technical-framework/latest/04_-_Attribute_Specification_for_the_Swedish_eID_Framework.html#attributes

users to prove who they are so they can find their pensions, and the PDP has chosen GOV.UK One Login to provide this service.[12] In future, the national digital ID could become an alternative to using One Login. If consumers will use their digital ID in future to set up and access pensions dashboards, we would encourage the government to consider whether any additional attributes, beyond name and date of birth, could help support this process, provided security and protection for the consumer is maintained.

The inclusion of a biometric facial image means it is important to recognise how different demographics can experience unfair and adverse outcomes when biometrics are used. For example, written evidence provided to the Parliamentary (Commons) Science and Technology Select Committee Inquiry on current and future uses of biometric data and technologies (2014) included citations of academic analysis that suggest biometric technologies "suffer from 'demographic failures', in which they reliably fail to identify particular segments of the population".[13] Furthermore, the 2023 study by the National Physical Laboratory (NPL)[14] aimed to evaluate whether there was any bias in the facial recognition technologies being used by the Metropolitan Police Service and South Wales Police.[15] The study found that there was a "statistically significant imbalance between demographics"[16] and that "it is more likely to incorrectly identify black and Asian people than their white counterparts on some settings".[17]

The government also needs to clarify whether there will be requirements to update the photo at regular intervals, comparable to the requirements to renew a photocard driving licence every 10 years with a recent photo.[18]

It is important to recognise the risks associated with certain mobile devices being less secure for facial recognition, as this could increase the chances of fraudsters being able to access and misuse consumers' digital IDs or carry out identity theft. Which? testing of mobile phones recently found that 'face unlock' on "many new smartphones from major brands can be bypassed using nothing more than a photo of the owner".[19] This bears on how consumers may create their national digital ID on their mobile devices (for example by taking a selfie photo and doing a liveness check). Similarly, consumers setting up a passkey to use facial

---

[12] Pensions Dashboard Programme (2024) *PDP confirms identity service provider*. Available at: https://www.pensionsdashboardsprogramme.org.uk/publications/news/pdp-confirms-identity-service-provider

[13] Dr Edgar Whitley (2015) *Written evidence to the Inquiry on Current and future uses of biometric data and technologies*. Available at: https://committees.parliament.uk/writtenevidence/53437/pdf/

[14] National Physical Laboratory (2023) *Facial Recognition Technology In Law Enforcement Equitability Study Final Report.* Available at: https://science.police.uk/site/assets/files/3396/frt-equitability-study_mar2023.pdf

[15] UK Parliament Post (2024) *Biometric data: Misuse, use, and collation*. Available at: https://researchbriefings.files.parliament.uk/documents/POST-PN-0731/POST-PN-0731.pdf

[16] Ibid.

[17] Rajeev Syal (2025) *Home Office admits facial recognition tech issue with black and Asian subjects.* The Guardian. Available at: https://www.theguardian.com/technology/2025/dec/05/home-office-facial-recognition-tech-issue-black-asian-subjects

[18] GOV.UK. *Renew your driving licence*: https://www.gov.uk/renew-driving-licence

[19] Which? (2026) *Why using face unlock on a phone could be risking your data.* Available at: https://www.which.co.uk/news/article/why-using-face-unlock-on-a-phone-could-be-risking-your-data-az8fe2G7uX8n

recognition to unlock the national digital ID could be vulnerable to a security risk on devices with insecure facial recognition. Conversely, restricting which devices can support the national digital ID may lead to forms of digital exclusion on the basis of skills or affordability. The government must clarify if this hardware-based risk is inside the scope of the cybersecurity standards of the DVSTF.

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

Which?'s customers can choose where they receive our products and services, and this may not be their billing address or residential address. For these reasons, we do not anticipate relying on customer residential address information provided through the national digital ID.

Nonetheless, there may be other potential consumer use cases where inclusion of address could be beneficial. For example, we are aware that Ofgem is developing the Consumer Consent Solution (CCS)[20], which intends to give consumers control over how their energy data is shared. Energy data is inherently related to a property, as opposed to specific attributes about the individual, and the consumer needs to be able to demonstrate that they are entitled to give consent to share energy data about that specific property. If addresses were included in the national digital ID, this could help consumers confirm that entitlement.

The Department of Business and Trade recently published Smart Data 2035, the government's Smart Data Strategy.[21] Smart data gives consumers the ability to share their data between businesses and other organisations, to enable new uses of data in ways that benefit consumers, society, and economy. Schemes enable consumers to have greater choice of innovative and personalised services (and could lead to better prices, for instance services such as automatic switching or tailored account management), but the schemes rely on verifying that the appropriate person has given consent for the data sharing. Digital ID could play a role in enabling smart data schemes through identity verification to prove entitlement to give consent. Consumer use cases that also involve verifying a property or a location associated with the consumer, such as smart data in the property sector, may also benefit from inclusion of address in a consumer's national digital ID.

The government will need to weigh this up against the downsides of including further personal data in the national digital ID. Address is an attribute likely to change more frequently over a lifetime than the others proposed for inclusion (such as name or nationality), which could lead to more administrative burden for both consumers and the government. Similarly, it will be important to ensure that including an attribute that may change more regularly does not lead to additional security risks and that the process to update addresses cannot be abused by fraudsters.

---

[20] Ofgem (2025) *Consumer Consent decision*. Available at: https://www.ofgem.gov.uk/decision/consumer-consent-decision

[21] UK Government (2026) *Smart Data 2035: The UK's Smart Data Strategy*. Available at: https://assets.publishing.service.gov.uk/media/69c11f9ed588c92c483e4b66/smart-data-strategy.pdf

3. **Businesses and organisations accepting the national digital ID need to trust that the information on it is up to date and accurate. We are exploring whether people with a digital ID should be legally required to inform the government within an appropriate timeframe of certain changes (such as a name change) or errors to their personal information, so that their digital ID can be updated. To what extent do you agree or disagree with a legal requirement to inform the government of changes or errors within an appropriate timeframe?**

It is important that the process to update one's national digital ID is proportionate and should not be more harsh or onerous than the existing processes for updating physical IDs.

We acknowledge that there are existing requirements to update driving licence details (name and address) and that there are penalties for not complying with these requirements. That is, a person can be fined up to £1000 for not notifying DVLA about an address or legal name change.[22,23] Individuals also have a legal requirement to keep their electoral roll details up to date and failure to do so can also be met with a fine.[24] The government's proposed national digital ID is optional, so placing a legal requirement to update it on consumers that sign up for it may diminish takeup. However, if details are not correct or up to date then relying parties cannot have confidence in using the national digital ID for ID or age verification. If relying parties do not trust the national digital ID and therefore do not offer the option to use it, consumers will be unable to experience the potential benefits, such as less friction, more convenience, speed of service and control over their own data.

In order to minimise the burden on consumers, we recommend that in consumer use cases the national digital ID is only required to be up to date at the point of use by the consumer.

The process for consumers to update their attributes within the national digital ID must be as straightforward, proportionate, inclusive, accessible and user-friendly as possible. This should include making it clear where in government to go to make the necessary changes. Consumers may not be familiar with GDS as the government department that owns the national digital ID product, as opposed to other government departments (such as HMRC or DWP) or local authorities that they may be more accustomed to dealing with when accessing public services. The government should consider if there are ways to link up across public services to streamline the process for consumers seeking to update their attributes.

Chapter 3.3: Utility in the wider economy

1. **The national digital ID would be useable across the private and public sectors, alongside other options like physical documents and other appropriate digital identities from third parties. To what extent do you agree or disagree that the**

[22] GOV.UK. *Change the address on your driving licence:* https://www.gov.uk/change-address-driving-licence
[23] DVLA. *Information on driving licences.* Available at: https://assets.publishing.service.gov.uk/media/688c6e8f6c7eb66caea94e04/ins57p-information-on-driving-licences.pdf
[24] You must register to vote if an electoral registration officer asks you to do so and you meet the conditions for registering. If you're asked to register and do not, you could be fined up to £1,000: https://www.gov.uk/electoral-register. Civil penalties can also be imposed for providing false information: https://commonslibrary.parliament.uk/research-briefings/sn06940/

private sector and third parties should be able to use the digital ID alongside other options?

It is important to maintain choice for consumers - both choice of different digital ID and DVS providers and choice between digital and non-digital ID options. If consumers do not want to use a particular provider or would prefer to use physical forms of ID, they should not be disadvantaged or experience worse outcomes.

To realise the potential impact for the economy of expanding the use of DVS, use cases must deliver real value to consumers in their everyday lives. Consumer outcomes from using DVS should be monitored, as well as monitoring consumer journeys. Simply monitoring initial uptake will not identify whether it is truly working for consumers, since uptake might also increase because of a lack of alternatives. For example, in the case of Open Banking, we and other experts have identified limited monitoring of consumer experiences, a lack of consumer protections and limited evaluation of consumer outcomes. While adoption rates for Open Banking are known, there is little insight into impacts on financial inclusion or consumer protection gaps.[25]

Part 4: Inclusive

Chapter 4.1: Eligibility for the digital ID

2. **Which of the following ages do you think is most suitable to access the digital ID system from? 16/13/birth/other**

We encourage the government to think about specific consumer use cases to determine the benefits or drawbacks of lowering the age of eligibility from the proposed age of 16. For example, allowing access to the national digital ID at the age of 13 could allow teenagers to show a digital ID at the cinema to see a film rated 12A or 15. Young teens are also unlikely to have any other forms of ID - they are too young for a driving licence or student ID and many may not have a passport, or may not have permission from a parent, guardian, or care-giver to take it to social events.

On the other hand, we note that Article 8 of the UK GDPR provides that only children aged 13 years and over may lawfully provide their own consent for the processing of their personal data in the context of an information society service (ISS).[26] While the national digital ID is not an ISS, it does raise questions about whether anyone under 13 could provide meaningful consent to the processing of their personal data from creating a national digital ID. Therefore, the national digital ID could conceivably be useful for consumers in their teens, but may be less feasible for consumers younger than this.

---

[25] Which? (2025) *GUEST ARTICLE: What should future smart data schemes learn from Open Banking?* Available at: https://www.which.co.uk/policy-and-insight/article/guest-article-what-should-future-smart-data-schemes-learn-from-open-banking-apo9z2q49CkM

[26] ICO. *What are the rules about an ISS and consent?* Available at: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/children-and-the-uk-gdpr/what-are-the-rules-about-an-iss-and-consent/

Chapter 4.2: Unlocking access across society & Chapter 4.3: Commitment to support inclusion

We support that the proposed national digital ID is no longer intended to be mandatory. We believe consumers should retain the right to choose whether or not they want to use it. We support the commitment to an inclusion programme. It is important that the introduction of the national digital ID does not increase digital exclusion for consumers. We are concerned that digital ID has the potential to lead to exclusion in two different ways.

Firstly, if people are already experiencing digital exclusion through lack of skills, affordability or a suitable device, or if they do not have physical forms of ID, then it may be very difficult for them to access the national digital ID. Secondly, people who do not have a national digital ID for any reason (including personal preference) may be excluded from products and services that use and rely on the national digital ID.

Barriers to consumers accessing the national digital ID include data affordability. Ofcom reports that 6% of consumers do not have internet access at home and that 19% of UK adults are smart phone only users.[27] UK mobile contracts are typically capped by data usage, so if a consumer uses up their data allowance this could have implications for their access to digital ID and the services that it supports. People without home internet access or with caps on their mobile data usage may instead use public computers (such as at libraries or community centres) to access digital services. However, it is not clear whether it would be possible for these people to verify a digital ID credential on a public computer or device.

One option to address some of the exclusionary impacts related to data costs might be to apply zero-rating of national digital ID applications and associated services. Zero-rating is when an ISP applies a price of zero to the data traffic associated with a particular application and the data does not count towards any data cap in place on the internet access service.[28] The government could consider engaging with ISPs on the scope to apply zero-rating to accessing the national digital ID or services that rely upon it. However, we note that this may be more straightforward for public sector use cases of the national digital ID than for consumer use cases. If the national digital ID is applied to consumer use cases across the wider economy in future, this could make it more complicated to implement zero-rating, particularly if these consumer use cases could also be accessed using alternative, private digital ID providers as this may raise competition issues (with the government's national digital ID product having an unfair market advantage through zero-rating).

Consumer willingness to use the national digital ID may also present a barrier and lead to exclusion in future, especially if national digital ID use becomes widespread enough that some relying parties stop accepting physical ID alternatives (this is discussed further below).

---

[27] Ofcom (2026) *Adults' Media Use and Attitudes Report.* Available at: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes-2026/adults-media-use-and-attitudes-2026-report.pdf?v=415430

[28] BEREC. *What is zero rating?* Available at: https://www.berec.europa.eu/en/what-is-zero-rating?language_content_entity=en

To mitigate the above risks of exclusion, we support the government's proposal to have alternative access routes, provided they are sufficiently secure. These alternative access routes should make it easier for consumers with fewer digital skills or without physical ID documents to access the national digital ID. However, to prevent people becoming excluded from other services, it is also important to ensure that use of digital ID does not become the only way for people to access certain services.

Which? has previously campaigned to protect free access to cash[29] for consumers who rely on it as many banks and free ATMs have been disappearing from local streets. Despite the success of this campaign – which resulted in the introduction of a robust legal framework to ensure that consumers and businesses can continue to access cash, even as the economy shifts toward digital payments – there are still plenty of shops that choose to only accept digital or card payments in store. LINK's recently published results from a survey on cash acceptance found that while 77% of retailers accept cash, 14% went cashless in the last year.[30] LINK (which runs the UK's ATM network) also published in 2024 that "50 per cent of people have recently been somewhere that did not accept or discouraged the use of cash, a 22 per cent increase on last year."[31] There could be a risk of further exclusion if retailers selling age-restricted products in future decide to only accept age verification via the national digital ID. We encourage the government to consider the longer-term risks as national digital ID takeup and usage expands and what this might mean for consumers who cannot or choose not to use the national digital ID.

Chapter 4.4: Accessibility

We support the government's efforts to make the national digital ID accessible for all consumers that want to use it. The design and delivery of the proposed national digital ID should have good outcomes for all consumers.

Chapter 4.5: Alternative access routes

We support the proposal for alternative access routes to enable all eligible consumers to access and use the national digital ID, even if they are not digitally literate or do not have a smartphone device. We agree that this could help contribute to greater inclusion and accessibility of the national digital ID, which will allow more consumers to experience the potential benefits from using it in consumer use cases. There are existing examples of non-digital access routes to engage with digital smart data schemes, which the government may be able to learn from. In Open Banking, the Financial-grade API (FAPI) security standard has a provision for a customer to provide consent and access their personal data by non-digital means.[32] This is predominantly designed for consumers who do not have

[29] Which? (2024) *How Which? campaigned to protect cash, and won.* Available at: https://www.which.co.uk/news/article/how-which-campaigned-to-protect-cash-and-won-aX7gJ2g0nH7x
[30] LINK (2026) *Keeping Choice Alive: Measuring Cash Acceptance on the UK High Street.* Available at: https://www.link.co.uk/media/a0knmcpw/link-cash-acceptance-report.pdf
[31] LINK (2024) *Half of UK adults say they've had issues paying with cash.* Available at: https://www.link.co.uk/news/half-of-uk-adults-say-they-ve-had-issues-paying-with-cash
[32] Open ID (2019) *OpenID Certification Program Expands with the Release of Financial-grade API Client Initiated Backchannel Authentication Profile (FAPI-CIBA) Certification.* Available at: https://openid.net/openid-certification-program-expands-with-the-release-of-financial-grade-api-

access to smartphones or computers. We encourage the government to look at examples like this when designing alternative access routes, but it is also vital that security is top of mind in the design process. We would caution the government to ensure that the alternative access routes are just as secure as the typical digital onboarding routes. This should involve checking that the onboarding process cannot be hijacked by fraudsters. We discuss this in more detail in our response under Part 5 below.

Part 5: Trusted

Chapter 5.1: Data protection and privacy & Chapter 5.2: Securing the national digital ID system

We support a number of the principles set out in the chapters 5.1 and 5.2, so we have combined our response to these chapters. The key point we would like to emphasise, in line with earlier comments, is that the national digital ID must meet at least the same standards as private providers certified against the DVSTF.

We support the approach of implementing privacy by design and default in the national digital ID. We also support the plans for data protection impact assessments (DPIAs) and would like to highlight the importance of compliance with data protection principles and legal requirements for building and maintaining consumer protection. This will be vital for building and maintaining consumer confidence and trust.

We note that the consultation mentions that "accuracy will be maintained via authoritative sources and user-friendly update mechanisms". It is important that the update process must be as straightforward and frictionless as possible for consumers using the national digital ID in consumer use cases. If this process is too difficult or complicated consumers may not engage with it, which will have follow-on effects of eroding the trust of other parties in the ecosystem (such as relying parties or the businesses they are providing services to), and the market will not be able to operate effectively.

We also support the principles of data minimisation and selective disclosure. DVS providers can adhere to data minimisation by giving consumers more control of how much data they share through selective disclosure. The principle of selective disclosure enables a consumer to show only the relevant attributes for a particular use case, as opposed to sharing unnecessary or irrelevant details, which is what can happen with physical IDs that often display multiple attributes at once. Which?'s policy work on smart data has highlighted the link between consumer control of how their data is used and shared, and consumer trust and confidence in engaging with smart data schemes.[33] Our research has also found that people want meaningful control over their data, but feel powerless to engage with organisations who collect and use their data because of the power imbalance between consumers and organisations.[34] Over the past two and a half years Which?'s Consumer Insight Tracker (a

client-initiated-backchannel-authentication-profile-fapi-ciba-certification/

[33] Which? (2025) Building consumer trust in Smart Data. Available at: https://media.product.which.co.uk/prod/files/file/gm-c8fb7d84-ecd4-43fd-89c4-38eadcfc7c83-building-consumer-trust-in-smart-data-1.pdf

[34] Which? (2018), *Control, Alt or Delete? Consumer research on attitudes to data collection and use*. Available at: https://www.which.co.uk/policy-and-insight/article/control-alt-or-delete-consumer-resear

monthly poll weighted to be demographically representative of the national population[35]) has consistently shown that the majority of consumers (between 60-67%) are worried about how data about them is collected and used by businesses.[36] The control the national digital ID proposes to offer consumers over how they use and share their identity data with relying parties and businesses may help build and maintain trust in these services.

We are supportive of plans to use cybersecurity best practice standards and to maintain high security standards through continuous improvement and responding to evolving threats. It is critical that consumers' personal data is sufficiently protected to mitigate the risk of the national digital ID becoming a vector for ID theft and fraud.

We reiterate that it is vital that public and private digital IDs offer the same standards of protection for consumers. Inconsistencies across the market may leave consumers exposed to inferior experiences or outcomes, affecting consumer trust in the market as a whole. We were therefore somewhat concerned that GOV.UK lost its DVSTF (formerly DIATF) accreditation in 2025.[37]

We have seen international examples of national digital IDs being subject to cyber attacks (such as Estonia[38] and India[39]), so are aware that the national digital ID could become a target. However, we note that the proposals intend for the national digital ID to be part of a decentralised data model (unlike the Aadhaar in India for example, which is a centralised model), which may help mitigate some of the risks.

Chapter 5.3: Fraud as a national challenge

1. **We want to ensure these alternative access routes are secure. What do you think are the most important factors we need to consider in order to achieve this?**
2. **What do you think are the most important factors to consider when ensuring**

---

ch-on-attitudes-to-data-collection-and-use-aTS7R0Z87AI2

[35] Which? (2024). *About the Consumer Insight Tracker.* Available at: https://www.which.co.uk/policy-and-insight/article/about-the-consumer-insight-tracker-asxTG8k9XrQW

[36] The survey question is: 'How worried are you, if at all, about how data about you is collected and used by businesses? Very worried, Fairly worried, Not very worried, Not at all worried, Not applicable, Don't know.' The proportion of consumers worried is calculated by adding the proportion of respondents that are Very worried or Fairly worried. Which? (2024), Consumer worries dashboard. Available at: https://www.which.co.uk/policy-and-insight/article/consumer-worries-dashboard-akJMn5c4FKMv

[37] ComputerWeekly.com (2025) *Gov.uk One Login loses certification for digital identity trust framework*. Available at: https://www.computerweekly.com/news/366623835/Govuk-One-Login-loses-certification-for-digital-identity-trust-framework

[38] e-Estonia (2021) *Estonian e-state has experienced several hacking incidents as of late: What are the lessons learned?* Available at: https://e-estonia.com/estonian-e-state-has-experienced-several-hacking-incidents-as-of-late-what-are-the-lessons-learned/

[39] Firstpost (2018) *Aadhaar security breaches: Here are the major untoward incidents that have happened with Aadhaar and what was actually affected*. Available at: https://www.firstpost.com/tech/news-analysis/aadhaar-security-breaches-here-are-the-major-untoward-incidents-that-have-happened-with-aadhaar-and-what-was-actually-affected-4300349.html

alternative access routes to the national digital ID are not misused by fraudulent actors?

It is vital that the government can ensure that both the alternative access routes and the typical digital onboarding process are secure and cannot be misused by fraudulent actors. Identity theft is a growing type of fraud, and a consumer's identity is extremely valuable to a fraudster, as it can be used to open credit in the consumer's name leaving the consumer to deal with the debt, or to take over the consumer's existing accounts. This can be extremely stressful for consumers who can end up with a lower credit score, locked out of their accounts, dealing with debt collectors and facing time-consuming processes to prove their innocence. Which? has seen cases where the repercussions can last for years.[40] We recommend that the government examine the onboarding process to obtain a digital ID from a fraudster's perspective and run 'red-teaming' exercises - that is, simulating an adversarial attack. It is important to identify any ways that a fraudster could effectively pretend to be someone else while creating a digital ID and then for the government to find ways to disrupt that process and make it impossible for the fraudster.

Red-teaming the onboarding processes should be done for all routes to access, not just the alternative access routes. However, it is especially important to examine how account security would work in a non-device based context. For example, with a smartphone, consumers can benefit from additional security via biometric passkeys (provided suitably secure devices are being used) or authenticator apps, but these measures may not be available for those using alternative access routes. The government must clarify how these alternative access routes will ensure the security of the accounts set up through this process.

Additionally, the government must consider how to mitigate the risk of fraudsters mimicking government communications about the national digital ID as part of a phishing campaign. This may require engagement with online platforms and telecoms companies to ensure they are blocking any material that is designed to imitate government communications. We note that efforts to date from industry to prevent fraudulent content from reaching consumers has had limited effect, as consumers are still regularly exposed to fraudulent content via online search, social media and SMS. For example, Which? recently reported on fake texts, calls and emails mimicking HMRC.[41] Which? also found that 170,000 HMRC scams were reported in the year to August 2025.[42] We therefore want to raise our concerns that industry-led efforts to mitigate against fraudsters mimicking government communications about the national digital ID are unlikely to be sufficiently effective to protect all consumers from receiving these fraudulent communications.

---

[40] Which? (2025) *Identity fraud: what to do if you're being chased for debt that's not yours*. Available at: https://www.which.co.uk/news/article/identity-fraud-what-to-do-if-youre-being-chased-for-debt-thats-not-yours-adTwq5b6N9Dy

[41] Which? (2025) *How to spot HMRC phone, text and email tax scams.* Available at: https://www.which.co.uk/consumer-rights/advice/how-to-spot-hmrc-phone-text-and-email-tax-scams-aktLy8n3sBWV

[42] Which? (2025) *HMRC warns of tax scams targeting self-assessment customers.* Available at: https://www.which.co.uk/news/article/hmrc-warns-of-tax-scams-targeting-self-assessment-customers-avRXQ5P0KQA7

Finally, we would like to understand what the government intends to happen when a user of the national digital ID dies. Considerations should include ascertaining the owner of the digital ID has died, and the process for what should subsequently happen to that digital ID. This may bear on the experiences of the person's loved ones or next of kin. The digital ID may have been used to unlock access to assets or services such as pensions, affecting the household as a whole. In other consumer use cases, access to the digital ID of someone who has died may also aid next of kin's ability to resolve or close accounts.[43] We note that there could also be fraud or security risks if digital IDs can be misappropriated after death, so would encourage the government to consider ways to mitigate this; for example, putting a 'deceased' flag on the digital ID, which may initiate additional checks or limit the circumstances in which that digital ID can be used.

Chapter 5.4: Ensuring strong oversight and governance

1. **What additional oversight mechanisms, if any, should be put in place for the national digital ID system?**
2. **What measures can you suggest, if any, that could be put in place to make sure people can resolve issues with their national digital ID?**

It is striking that redress is mentioned just once in the consultation document. Redress is an important outcome for consumers in well-functioning markets. It incentivises the prevention of harms by businesses and gives consumers confidence to engage in the market

When a consumer is engaging with the national digital ID, they may often be expecting a service from the relying party that requires a DVS transaction. The consumer is then likely to go directly to the relying party if something goes wrong when they are using the digital ID.

We would recommend that the government monitor consumer outcomes as usage of digital ID grows and revisit whether new or additional redress routes are required if consumers are experiencing harms that are specific or unique to the digital ID market.

Part 6: Wider summary of impacts

This chapter references potential impacts on existing DVS providers, as the national digital ID could lead to some displacement in the digital ID sector if the national digital ID functions as a close substitute for services currently supplied by private DVS providers.

The consultation document includes questions about other benefits and costs to businesses and households from introducing the national digital ID system, but does not ask about the impact for consumers. The consultation document refers to broader use cases in the wider economy beyond public services, such as proving age when purchasing alcohol, yet consumers are not explicitly mentioned at all. We find this lack of recognition of consumer interests and consumer perspectives concerning, given the government is also suggesting that the national digital ID could end up being used in consumer use cases.

[43] Which? Magazine (September 2024) *How to plan for your digital death*.

We believe there could be risks to consumers from the proposed mixed landscape with multiple certified private DVS providers operating alongside a government-owned digital ID product. Before the government's announcement in September 2025 to propose a national digital ID, the UK's ID landscape consisted of multiple private DVS providers. The proposals in the consultation will move the UK into a mixed landscape with a government-owned national digital ID (which may be the only option for some use cases, like accessing public services) operating alongside industry offerings. Superficially this appears to increase the choices available to consumers, but if the national digital ID does not at least meet the standards of certified industry providers, this is likely to contribute to consumer confusion about what to expect when they engage with the market. It is therefore vital that the national digital ID is certified against the DVSTF.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:
Stephanie Borthwick
Principal Policy Adviser
stephanie.borthwick@which.co.uk

May 2026