

UK Government Digital ID Consultation Response

Submitted by Toby Bolton, founder of .zkdid™

Expert response in a personal capacity | 28 April 2026

Respondent	Toby Bolton
Capacity	Expert response in a personal capacity
Relevant work	Founder of .zkdid™, an open-source public-good decentralised identity and trust-root initiative
Primary concern	To ensure national digital ID empowers citizens without becoming a mandatory surveillance or permissioning layer

Executive summary

I support the objective of making public services easier, reducing repeated identity checks, reducing fraud and allowing people to prove only what is necessary. However, that support is conditional. A national digital ID must not be treated simply as a government technology project. It touches something deeper than administrative identity. It touches personhood, civil liberty, trust, autonomy and the relationship between the citizen and the state.

The government should recognise that a government-issued digital ID can be useful for government services, but it should not become the foundation of a person's entire digital life. A passport, driving licence, visa or right-to-work credential can help prove official facts. It should not become the authoritative layer through which a person must be recognised, checked or permitted to act in ordinary society.

The central risk is the trust paradox. The more useful and powerful a digital identity system becomes, the more dangerous it becomes if the root of trust is controlled by a single institution. A system presented as optional and convenient can gradually become mandatory in practice through employment, banking, housing, age checks, online safety, retail, public services and private-sector adoption. At that point, digital ID stops being a tool for the citizen and becomes a permissioning layer over ordinary life.

The government should therefore avoid becoming the root of digital personhood. A government credential can be valuable, but it should sit above an independent public-good identity and personhood infrastructure that keeps citizens in control. The system should enable privacy-preserving decentralised identity and proof-of-personhood approaches, including systems such as .zkdid™, rather than requiring every everyday interaction to call back to the state or to a government-approved checker.

This distinction matters most when considering revocation, exclusion and control. A passport, visa, driving licence or right-to-work credential may need to be suspended or revoked in lawful circumstances. A person's ability to exist digitally, prove uniqueness, access essential services and

participate in society must not be revocable by a single institution. Government credentials are not the same thing as personhood.

The strongest model would allow government digital ID to help citizens onboard into a wider privacy-preserving identity ecosystem, while leaving citizens in control. Used in this way, GOV.UK digital ID could strengthen public services without becoming an internal passport for everyday life. It could help verify official facts while allowing independent public-good infrastructure to carry the wider burden of trust, privacy, selective disclosure and user sovereignty.

The system should therefore be built around data minimisation, open standards, selective disclosure, zero-knowledge proofs where appropriate, local or device-side proof generation, unlinkability between contexts, independent oversight, meaningful redress and a permanent right to use non-digital alternatives.

About the respondent and .zkdid™

I am Toby Bolton, founder of .zkdid™, a British open-source public-good initiative developing a decentralised, zero-knowledge, DNS/DID-style trust-root architecture for people, devices and organisations.

.zkdid™ is intended to address what may be described as the trust paradox in digital identity. Society needs stronger trust online, especially in an age of AI, deepfakes, fraud, synthetic accounts, automated agents and increasingly complex machine-to-machine interactions. However, if the root of digital trust is controlled by one government, one large technology platform, one bank, one vendor or one foundation, public trust can quickly erode. The more powerful the identity system becomes, the more important it is that the root is insulated against capture, abuse, coercion, monopoly control or quiet repurposing by future institutions, governments or automated systems.

The purpose of .zkdid™ is to explore that safety layer before digital identity becomes too deeply embedded to correct. Powerful identity infrastructure should not be built on the assumption that every future government, institution, vendor or automated decision-making system will remain benign. It should be designed so that citizens retain agency, control and meaningful choice. In a properly sovereign model, people should control their own keys, proofs and disclosures wherever possible, rather than depending on any single institution to recognise, permission or revoke their digital existence.

.zkdid™ explores a sovereign, decentralised trust layer that could allow proof of personhood, credential verification and selective disclosure without exposing unnecessary personal information. Its DNS/DID-style architecture is important because DNS remains one of the core coordination layers of the internet. By building with DNS concepts, decentralised identifiers and open standards in mind, .zkdid™ aims to be backwards-compatible with existing internet infrastructure while creating a more privacy-preserving trust layer for the future.

The intention is not to replace government-issued credentials such as passports, visas, driving licences or right-to-work status. The intention is to ensure those credentials can support a wider privacy-preserving architecture without making the government the routine gatekeeper for everyday digital life.

A government digital ID can help prove official facts. It should not become the root through which all digital personhood, access and participation must be mediated.

This response is therefore not a procurement pitch. It is a public-interest architectural response. The government digital ID could be valuable if it is designed as one credential within a broader open ecosystem. It would be dangerous if it becomes the universal root of identity, the default checker for private-sector life, or a single identifier that follows a person everywhere.

Digital identity is not benign simply because it is convenient. It can reduce fraud, improve services and protect privacy if designed well. But if designed badly, it can create lasting mechanisms of control over citizens, especially if it becomes mandatory in practice or embedded into employment, finance, housing, public services and online life. A democratic society should therefore build digital identity with safety, restraint, openness and citizen sovereignty at the core.

Core principles recommended for the national digital ID system

- Empowering, not oppressive: the system must make life easier without making citizens feel watched, managed or permissioned.
- Optional in law and optional in practice: digital ID must not become mandatory through right-to-work rules, private-sector norms, banking, housing, online safety, employment platforms or access to public services.
- Government credentials are not personhood: official credentials may be revoked, but digital personhood and basic participation in society must not be revocable by a single authority.
- No routine call-home model: checks should avoid creating centralised logs of where, when and why a person proves something about themselves.
- Data minimisation by design: relying parties should receive the minimum necessary proof, for example over-18, eligible to work or credential valid, rather than full name, date of birth, address, nationality or biometric data unless strictly required.
- Selective disclosure and zero-knowledge proofs: privacy-enhancing technologies should be central, not treated as optional future improvements.
- Open standards and interoperability: citizens should not be locked into one government app, one vendor wallet or one commercial verification stack.
- Independent oversight and redress: revocation, suspension, matching, data sharing, biometric errors and account recovery must have rapid human review, clear appeal rights and public accountability.
- Permanent non-digital alternatives: no person should be excluded from work, housing, health, travel, money, public services or ordinary life because they do not have a smartphone or do not wish to use a digital ID.

Responses to consultation questions

The following answers follow the consultation structure. Where a single-choice answer is required, I have included the answer I consider most appropriate, followed by the reasoning.

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

The main potential benefits are reduced duplication, less paperwork, fewer repeated identity checks, better fraud prevention and more convenient access to public services. A well-designed digital ID could also reduce the amount of personal information people disclose in daily life, especially where only a narrow attribute needs to be proven.

However, those benefits only exist if the architecture is privacy-preserving and trusted. The national digital ID should be treated as one useful source of official truth within a wider trust ecosystem, not as the whole identity system itself. It can help prove government-issued facts, but it should not become the foundation through which everyday life is authorised.

If the system becomes a state-centred identity layer used across ordinary life, it risks producing the opposite effect: public resistance, reduced trust and a fear that digital identity is being used as a control mechanism rather than as public infrastructure.

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

The main drawback is the risk of function creep. A system introduced for convenience and public services could gradually become the default means of accessing work, banking, housing, retail, online services, travel, age-restricted goods and public benefits. Even if the system remains optional in law, it may become mandatory in practice.

There is also a major trust issue. Many citizens are wary of centralised databases, government data leaks, opaque technology procurement and the possibility that emergency powers or future governments could repurpose digital infrastructure. If the public believes the system is a surveillance layer, resistance will be immense.

A further drawback is institutional, commercial and technical capture. If the system depends on a small number of approved wallet providers, checkers, cloud vendors, biometric providers or automated decision-making systems, public infrastructure could be shaped by commercial incentives, lobbying pressure or technical dependency rather than citizen rights.

1.0.Q3. To what extent do you agree or disagree that the proposed system could make it easier for people to prove who they are?

Answer: Somewhat agree, but only with substantial safeguards

I agree with the aim. People should not have to repeatedly produce passports, driving licences, utility bills or photocopies of sensitive documents. Digital proofs can make identity easier and safer.

However, I only agree conditionally. The government system can be a valuable source of official facts, but it should enable a wider, more sovereign identity ecosystem rather than dominate it. The strongest model would allow citizens to use government-issued credentials to support privacy-preserving proofs across trusted systems, without requiring the government to sit behind every interaction.

The system must not require a government app or government checker to sit behind ordinary life.

Proving age at a bar, eligibility for a service, or identity in a low-risk setting should not become a moment where the citizen appears to seek permission from the state. The right architecture would allow government credentials to support privacy-preserving proofs, while daily verification happens through user-controlled, device-local and interoperable mechanisms wherever possible.

1.0.Q4. Which public services would you want the government to prioritise making faster or more efficient using the system?

The highest priorities should be services where people already face serious friction or exclusion: benefits, pensions, health-related entitlements, childcare support, housing support, disability support, student finance, driving licence renewal, passport renewal, name changes and power of attorney.

The initial focus should be public service improvement, not making the government credential the default identity layer for retail, leisure, financial products and online life. The government should avoid using the digital ID as a broad private-sector permissioning layer.

In the longer term, the UK should think beyond a single government ID app. The future trust problem includes AI agents, deepfakes, synthetic accounts, fraudulent phone calls, fraudulent emails and machine-to-machine interactions. That requires an identity and trust infrastructure that works across the internet while preserving privacy.

Government credentials can help onboard people into such a system, but they should not become the whole system. The government should encourage a wider trust framework that is open, interoperable, privacy-preserving and citizen-controlled, rather than one dominated by a single state credential, vendor wallet or checker service.

Part 2: Our approach

Chapter 2.1: Creating the digital ID

2.1.Q1. Are there technical issuance standards, beyond those already used by the GOV.UK Wallet, that should be used?

Answer: Yes

The system should be built around open, interoperable, privacy-preserving standards. Relevant areas include W3C Verifiable Credentials, Decentralised Identifiers, selective disclosure credentials, privacy-preserving credential status mechanisms, hardware-backed device security, secure recovery and revocation mechanisms, and strong cryptographic auditability.

OpenID-based credential protocols, including OpenID for Verifiable Credential Issuance and OpenID for Verifiable Presentations, may be useful where they support interoperability. However, they should not be treated as sufficient on their own. Any OpenID-based implementation must be carefully constrained so that it does not recreate a centralised identity-provider model, routine verifier-to-issuer tracking, or a dependency on a small number of dominant wallet, checker or identity providers.

The government should also design for post-quantum readiness. That does not mean prematurely deploying immature cryptography, but it does mean avoiding architectures that will be difficult to migrate. A credible roadmap should consider post-quantum safe signatures, post-quantum credential verification, crypto-agility and research into post-quantum zero-knowledge proof systems where appropriate.

Most importantly, the design should avoid routine online verification that creates transaction logs. The goal should be privacy-preserving proof, not a system where every relying party causes a check that can reveal where a person is, what they are doing and which services they are accessing.

2.1.Q2. Do you have concerns about the impact of the national digital ID specific to your part of the UK?

Answer: England

England has a strong tradition of individual liberty and resistance to compulsory identity infrastructure. A national digital ID stored on a phone 24 hours a day may feel intrusive to many people, especially if it becomes associated with employment checks, age checks, retail access and access to public services.

There is also a psychological and constitutional concern. A personal phone is not state property. Citizens should not feel that by carrying a government digital ID they have placed part of their private device under government observation, control or implied authority. The app or wallet must therefore be designed with no hidden monitoring, no unnecessary background activity, no excessive permissions, no behavioural telemetry and no sense that the state is occupying the citizen's device.

To earn trust, the system must be designed so citizens can clearly see that it is not a digital internal passport. It must not create a culture where people feel guilty until digitally verified. The government should legislate for meaningful alternatives and ensure that the digital ID does not become a practical requirement for ordinary life.

Chapter 2.2: Storing, managing and using the digital ID

2.2.Q1. Are there ethical factors government should consider when an individual deletes their digital ID?

Answer: Yes

Deletion must be a genuine right. A person should be able to remove the digital ID from their device without being penalised or quietly excluded from services. Deleting the credential from a device should not be treated as suspicious behaviour.

Deletion should mean effective deletion. If a person removes the digital ID, the credential material, device bindings, cached tokens, local identifiers, telemetry, usage metadata and recovery artefacts should be removed or cryptographically destroyed wherever technically possible. The system should not leave dormant tracking components, hidden profiles or practical traces that allow continued monitoring after deletion.

The government should clearly explain what deletion means. If underlying records are retained by departments, the user must understand that deleting the wallet credential is not the same as deleting government records. There should be clear routes to object to processing, correct errors and understand retention periods.

2.2.Q2. Are there ethical factors government should consider when revoking or cancelling an individual's digital ID?

Answer: Yes

Revocation is one of the most sensitive parts of the entire proposal. Revoking a passport, visa, driving licence or right-to-work credential may be lawful and necessary in specific circumstances. Revoking a person's broader digital personhood or ability to participate in society must never be possible.

If the digital ID becomes necessary for employment, banking, public services, online access, payments or essential goods, revocation could become a form of digital exclusion. Even if that is not the intention, the architecture could make it possible. That risk needs to be designed out from the start.

Personhood is not the government layer. A citizen has digital rights that sit alongside human rights, including the ability to access essential services, seek redress, communicate, participate and prove basic facts without being made dependent on a single revocable state credential.

Revocation must therefore be narrow, appealable, time-limited, transparent and subject to independent oversight. There must be emergency access routes where a person is wrongly locked out. No revocation decision should prevent access to essential services, healthcare, food, housing, legal rights or basic participation in society.

The key principle is this: official credentials can be revoked, but personhood must not be revocable.

2.2.Q3. Should people be able to store their national digital ID in holder services other than the GOV.UK Wallet, if certified to government standards?

Answer: Yes

Yes. Wallet choice is essential to trust and competition. Many citizens will resist a single government app as the only route. Certified holder services should be allowed if they meet strong security, privacy, accessibility and interoperability standards.

However, certification must not become a closed market that favours only a few large vendors. The system should support open standards, independent security review and portability. Over time, identity may become device-native and operating-system native rather than app-native.

The design should anticipate that future rather than locking the UK into one wallet model.

A sovereign, user-controlled trust layer should also be able to function with or without a government credential enabled. Government credentials can help prove official attributes, but they should not be confused with the user's underlying personhood or digital agency.

2.2.Q4. Should a government checker service be made available for private and third sector use at low or no cost?

Answer: Somewhat agree

There may be a case for a basic low-cost checker to prevent visual inspection fraud and support low-volume public-interest use cases. However, this must be tightly limited.

The danger is that a checker becomes a routine call-home mechanism. If every check creates logs of who checked whom, when, where and for what purpose, the checker becomes a surveillance risk even if the original intention is benign. Metadata can be as revealing as the identity data itself.

Where any phone-home or online status check is unavoidable, it must be designed to be immensely privacy-preserving. The system should minimise what the government sees, minimise what the verifier receives, and avoid creating a linkable trail of a citizen's activity.

The checker should therefore be designed for minimal disclosure, minimal logging, strong purpose limitation and user visibility. Wherever possible, it should enable a one-time or occasional verification that allows the user to generate privacy-preserving proofs locally thereafter, rather than requiring the government to be queried at every point of use.

2.2.Q5. Are there specific limitations that should be set for the government checker?

Answer: Yes

The government checker should be limited by design. It should verify only what is strictly necessary for the relevant use case. It should not become a general-purpose private-sector identity oracle.

Suggested limitations include: no routine tracking of relying-party use, no use for behavioural profiling, no commercial resale of verification metadata, no general-purpose unique identifier exposed to private

parties, no mandatory use where privacy-preserving alternatives exist, clear usage logs visible to the citizen and strict limits on retention.

The checker would be far safer if checks could be made unlinkable or anonymous wherever possible. The government should explore privacy-preserving status checks, anonymous credentials, blind-signature-style mechanisms, zero-knowledge proofs and status-list approaches that allow validity to be checked without revealing every use of the credential back to the issuer. W3C's Bitstring Status List, for example, is specifically framed as a privacy-preserving way to publish suspension or revocation status for verifiable credentials.

The checker should be framed as a verification tool controlled by law and citizen rights, not as an identity control point.

Part 3: Useful

Chapter 3.1: Information contained in the digital ID

3.1.Q1. What further information, if any, should the digital ID include?

The core credential should contain as little information as possible. I would not support expanding the core digital ID beyond what is strictly necessary at launch.

A national digital ID must not become a container for a person's full life profile. There is a clear difference between helping a citizen prove a narrow fact and creating a system that gathers identity, address, nationality, work status, benefits, qualifications, criminal record indicators, health-related eligibility, transaction history or service usage under one roof. The latter would create an unacceptable cybersecurity, civil liberties and trust risk.

Where additional attributes are required, they should be separate optional credentials, not part of one ever-expanding national identity profile. For example, proof of address, professional status, right-to-work conditions, educational qualifications, benefits eligibility or DBS-related information should be handled through separate, purpose-specific credentials with explicit consent, selective disclosure and strict purpose limitation.

Data should be minimised through architecture, not only through policy. Wherever possible, sensitive facts should be proven using derived credentials, local device-side proofs, zero-knowledge proofs, selective disclosure, pairwise identifiers and privacy-preserving verification. The relying party should receive the answer it is legally entitled to receive, not the underlying personal history.

The issuing process may need to consult authoritative government records, but that does not mean all those records should be stored in, exposed by or routinely carried within the digital ID. The safest system is one that allows a person to prove necessary facts without centralising unnecessary data.

3.1.Q2. If an organisation were to rely on address information, what would help it trust an address on the digital ID?

Address should not be part of the core national digital ID by default. Address is highly sensitive because it can reveal location, domestic circumstances, vulnerability, financial status and patterns of life.

If proof of address is offered in future, it should be a separate optional credential with freshness indicators, source confidence, expiry, revocation status and user consent at the point of disclosure. Relying parties should receive only the proof they need. For example, proof of residence in a local authority area may be enough, rather than full address disclosure.

Government should avoid building a single national database that combines biometric identity, address, nationality, identifiers and transaction history. That would create a major cybersecurity and civil liberties risk.

3.1.Q3. Should people with a digital ID be legally required to inform the government of changes or errors within an appropriate timeframe?

Answer: Strongly disagree

A legal obligation would undermine the claim that the system is voluntary. It would also create anxiety and potential penalties around what is supposed to be a citizen-centred convenience tool.

People should be encouraged and supported to keep information up to date, especially where the information affects a right or entitlement. However, creating a new legal duty risks turning the digital ID into a state-managed status system.

This would reduce trust and disproportionately affect people with complex lives, mental health issues, disability, domestic abuse risks, homelessness, caring responsibilities or limited digital access.

Where accuracy matters, the burden should primarily sit on service design, clear prompts, easy correction and proper departmental processes, not punitive obligations on citizens.

Chapter 3.2: Transforming public services

3.2.Q1. Are there barriers or inefficiencies that prevent people from interacting with public services that digital ID could help with?

Answer: Yes

Yes. Public services often require repeated identity checks, repeated explanations, different reference numbers, different passwords, long phone calls and confusing document requirements. A privacy-preserving digital credential could reduce friction.

However, the solution should not simply be to centralise more data. A better approach is to let people prove narrow facts when needed. For example, a person should be able to prove eligibility, age, residence in a region or relationship to a child without disclosing unrelated information.

Digital ID should be designed as a proof layer, not a profiling layer. Public services may need to know that a person is eligible for a service, but they do not always need to see the full set of records behind that eligibility. Where possible, the citizen should be able to grant a specific, time-limited and purpose-bound authorisation for a service to check only what is necessary.

For phone-based or remote support, the future should include cryptographic trust at the device and network level. A user could authenticate locally on their device and selectively disclose a proof during a call or online session without verbally answering weak security questions.

3.2.Q2. Have you faced issues knowing which public services are available based on your circumstances?

Answer: Yes

Yes. Government services are often difficult to navigate. People may not know what they are entitled to, which department is responsible, what evidence is required or how different services interact.

Digital ID may help with signposting, but the government should be careful not to make personalisation dependent on broad data sharing. It should be possible to provide better guidance without building a comprehensive profile of every citizen's circumstances.

Personalisation should be citizen-led wherever possible. A person should be able to ask, "what might I be eligible for?" without automatically giving government or third parties permission to construct a permanent, cross-service life profile.

3.2.Q3. Have you had difficulty accessing a public service because you were unable to prove identity?

Answer: Yes

Yes. Identity checks can be inconsistent, especially where services rely on knowledge-based questions such as historic addresses, first pet names or other memorable information. These methods can be confusing, insecure and inconsistent across platforms.

A privacy-preserving digital proof system could reduce these weak checks. The design should focus on proving the minimum necessary fact rather than repeatedly collecting and storing personal information.

3.2.Q4. Do you agree with adopting a method to identify and match people across different public services?

Answer: Somewhat disagree

I understand the administrative argument for matching people across services, but this is one of the highest-risk areas of the proposal. A universal identifier or similar approach can become a population-scale tracking tool if not strictly limited.

The government must be careful not to move from identity verification into general life profiling. Matching across services may sometimes be lawful and necessary, but it should never become a default mechanism for building a complete picture of a person's life, movements, entitlements, vulnerabilities, employment, family circumstances and service usage.

The future should not be based on large centralised databases of personally identifiable information. It should use privacy-preserving matching, pairwise or sector-specific identifiers, selective disclosure, access controls, audit logs and strict legal purpose limitation.

Departments should not automatically gain broad visibility into a person's interactions elsewhere in government. Matching should be need-based, lawful, transparent and proportionate. Citizens should be able to see when their data has been used to match them across services, except in narrowly defined lawful investigation contexts.

Where matching is not strictly required by law, the preferred model should be citizen-authorised access: specific, time-limited, purpose-bound and revocable wherever possible.

3.2.Q5. What ethical issues arise when designing a way to identify and match people across services?

The main ethical issues are surveillance, loss of context, function creep, error propagation, exclusion, biased matching, overreach, poor consent and weak redress.

The deeper ethical risk is that a system designed to identify people for services gradually becomes a system for analysing people across society. Identity infrastructure must not become a general citizen intelligence layer. It should help people access rights and services, not make every interaction part of a permanent state-centred profile.

A mistake in one system must not spread silently across government. A person wrongly matched, wrongly flagged, wrongly denied access or wrongly treated as fraudulent must have a rapid human route to correction.

The ethical principle should be: match only when necessary, disclose only what is necessary, retain only what is necessary and make the citizen's rights clear.

3.2.Q6. What technical issues need to be considered when designing a way to correctly identify and match people across public services?

The technical design should avoid one universal identifier used everywhere. It should consider pairwise identifiers, sector-specific identifiers, privacy-preserving record linkage, cryptographic proofs, secure enclaves where appropriate, strong access controls, tamper-evident audit logs, user-visible data access records and independent technical audits.

The system should also be resilient against biometric errors, account recovery attacks, device loss, SIM swap attacks, coercion, domestic abuse misuse, insider threats, vendor compromise and cloud provider dependency.

Data should be decentralised where possible. The more sensitive data is pooled into centralised systems, the higher the impact of a breach. Selective disclosure and zero-knowledge proofs should be used wherever they can reduce data sharing without reducing trust.

Technically, the system should favour proof over access. In many situations, a service does not need direct access to the underlying record. It needs a reliable proof that a condition is met. This distinction is crucial. A proof-based architecture protects citizens better than a lookup-based architecture.

Chapter 3.3: Utility in the wider economy

3.3.Q1. Should the private sector and third parties be able to use the digital ID alongside other options?

Answer: Somewhat disagree

I do not object to privacy-preserving digital proof being used in the wider economy. I do object to the national government digital ID becoming the routine identity layer for private-sector life.

This is the scenario many citizens will fear: a government-linked credential being needed to buy age-restricted goods, enter venues, collect parcels, join a gym, use online services, rent property, open accounts or participate in ordinary life. Even if technically optional, market behaviour can make it practically mandatory.

The better model is for government credentials to support issuance of privacy-preserving, user-controlled derived proofs. The relying party should not need to know more than the relevant fact. In many cases, it should not need to know that a government credential was the original source of trust at all.

The private sector should never be allowed to demand more personal information than is required for the transaction, and it should not be allowed to use digital ID as a general tracking or profiling mechanism.

Private-sector access should be subject to strict purpose limitation, transparency, citizen control, auditability and penalties for misuse. No business should be able to turn digital ID into a condition of participation where a less intrusive proof would be sufficient.

Chapter 3.4: Tackling illegal working

3.4.Q1. Are there additional challenges businesses would face in carrying out fully digital right-to-work checks for all new workers?

Answer: Yes

Yes. Fully digital right-to-work checks could create cost, training, access and liability burdens for businesses, especially small employers. It could also exclude people who have difficulty with digital systems or whose records are wrong or delayed.

There is also a trust risk in positioning national digital ID primarily through the lens of illegal working. That framing may make the public feel the system is about enforcement rather than empowerment. Right-to-work checks are important, but they should remain a specific credential and process, not the justification for a broad identity layer across society.

Different jobs require different checks. A basic right-to-work check is not the same as a criminal records check, professional qualification check, safeguarding check or immigration condition check. These should be separate, purpose-specific credentials or checks rather than rolled into one powerful identity system.

3.4.Q2. Would additional support be required for business to comply with fully digital right-to-work checks?

Answer: Yes

Businesses would need clear guidance, low-cost access, support for small employers, staff training, fallback routes, fraud guidance, accessibility guidance and clear liability rules. There must also be a route for workers whose digital record is wrong or whose device is lost, broken or unavailable.

No person should lose employment or be unable to start work because of a technical failure, account recovery issue, device problem or government data error.

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

An organisation should receive only the minimum lawful confirmation required: that the check was completed, that the person has the right to work, any relevant work conditions or expiry date, and an audit reference sufficient for compliance.

The employer should not receive unnecessary underlying personal information. Criminal records or safeguarding checks should not be bundled into the general right-to-work process unless the role lawfully requires a separate check.

A right-to-work check should remain a narrow compliance proof. It should not become a gateway into wider personal information about the worker's identity history, immigration background, family circumstances, benefits, housing, health, criminal record or broader government profile.

Part 4: Inclusive

Chapter 4.1: Eligibility for the digital ID

4.1.Q1. Are there any other groups that should be included?

Answer: Yes, with safeguards

Eligibility should broadly align with people who need to prove identity, status or entitlement in the UK. However, special care is needed for children, vulnerable adults and people who cannot consent independently.

For children, any digital identity or age-assurance function should be parent- or guardian-controlled, age appropriate and strictly minimised. A child should not be placed into a lifelong behavioural identity system simply because online safety requires age assurance.

There is a legitimate need for privacy-preserving age proofs online. However, government digital ID is not necessarily the right mechanism for routine child age verification across the internet. If government credentials become the default route for online safety, there is a risk that children's digital lives become indirectly supervised through state-linked identity infrastructure.

The better model is local, selective and protective. Parents or guardians should be able to help a child prove age or eligibility without creating a centralised trail of browsing, service access or online behaviour. Public-good identity infrastructure, including decentralised proof-of-personhood systems such as .zkdid™, could help support parent-linked or guardian-controlled proofs from the root, without requiring constant government identity checks across a child's online life.

The government should not use online safety as a back door into normalising state-linked digital identity for children. Child protection must not become child tracking. The aim should be safety with privacy, not safety through constant identity exposure.

4.1.Q2. Which age is most suitable to access the digital ID system from?

Answer: Other

There should not be one simple age answer for all use cases. A child may need a parent-controlled proof for online safety or public services long before they are old enough to control a full national digital ID. A young person may need to prove age or right to work before adulthood. Full independent control may be more appropriate at 16 or 18 depending on the legal context.

The important principle is that child identity systems must be protective, minimal and controlled by appropriate safeguards. They must not normalise lifelong state-linked tracking from birth.

Government should not become the parent, guardian or routine supervisor of a child's digital life. That would be an overreach of the technology and would likely create distress, distrust and resistance among families. Where age assurance is needed, the system should favour parent- or guardian-mediated proofs, local device-side proofs, privacy-preserving credentials and independent public-good trust layers, rather than routing children's ordinary internet activity through government identity infrastructure.

Chapter 4.2: Unlocking access across society

4.2.Q1. Are there other barriers to creating or using the national digital ID?

Answer: Yes

Additional barriers include mental health issues, disability, lack of capacity to consent, domestic abuse, coercive control, homelessness, unstable housing, lack of documents, lack of smartphone access, poor connectivity, language barriers, distrust of government, fear of immigration consequences, age-related digital exclusion and past fraud or account compromise.

There is also a human barrier that should not be underestimated. For some people, digital systems do not feel empowering. They feel confusing, stressful, intrusive or anxiety-inducing. People with cognitive difficulties, trauma, serious anxiety, neurodivergence, illness or limited digital confidence may find a government identity app deeply uncomfortable rather than convenient.

A national system should therefore be designed around simplicity, restraint and choice. The government should not assume that more digital steps automatically mean better access. For some citizens, a digital ID will create a new barrier rather than remove an old one.

Device loss and account recovery are also major barriers. A person who loses a phone must not lose access to work, benefits, healthcare or essential services.

4.2.Q2. What additional support would help people use the national digital ID?

Answer: Yes

People will need in-person support, local trusted support, telephone support, accessible guidance, multilingual support, support for carers, support for people with disabilities, support for those without devices and urgent recovery routes where access is lost.

The government should be honest about cost. A system described as free to citizens still requires public funding, training, support staff, security operations, accessibility provision, appeals, recovery processes and ongoing maintenance. These costs should be assessed transparently.

There is also a democratic fairness issue. Taxpayers may be funding a system that many citizens do not want, do not trust or do not intend to use. That makes it even more important that the system is simple, proportionate and restrained. If the technology is made so complex that it requires large permanent support structures for millions of people, that is a warning sign about the design.

The best support is not only more helpdesks. It is better architecture: fewer steps, less data collection, less dependency on smartphones, clear opt-out rights, strong offline routes and systems that do not punish people for choosing not to participate.

4.2.Q3. Are there other groups at risk of ID or digital exclusion?

The consultation already identifies many relevant groups, including people on low incomes, people with poor connectivity, people lacking digital skills, older people, children, care leavers, people with disabilities, survivors of domestic abuse, people with limited English, people without stable addresses, people affected by trafficking or modern slavery, people in refuges or safe houses, trans and non-binary people, people with mismatched records, people in prison or recently released, people in hospitals or care homes, cultural communities with lower engagement in mainstream systems and people with privacy or security concerns.

I would add that the government should not treat reluctance as ignorance. Some people will reject digital ID not because they lack skills, but because they have principled concerns about privacy, surveillance, dependency, psychological wellbeing or the role of digital technology in ordinary life.

The system must not treat digital exclusion as a temporary inconvenience. For many people, non-digital routes will remain essential. For others, avoiding digital systems will be a legitimate personal choice. Both groups should be protected.

Chapter 4.3: Commitment to supporting inclusion

4.3.Q1. What support should be available to people who do not have a digital device?

People without a smartphone or tablet should be able to use passports, driving licences, physical documents, assisted verification, local public-service support and secure non-smartphone alternatives where appropriate.

No person should be required to own a smartphone to prove who they are. A human being's access to society must not depend on a private device, a battery, an app store, a vendor account or a mobile operating system.

The right to live without a digital device should be treated as a serious civil-liberties safeguard. Digital participation may be useful, but it should not become a condition of full participation in society. Some people cannot use digital devices. Some cannot afford them. Some do not trust them. Some may simply wish to live a more analogue, private or non-digital life. That choice should be respected.

Paper, physical and assisted routes should be protected in law, not merely offered as temporary transitional arrangements. They should remain available, affordable, dignified and practically equivalent.

4.3.Q2. How else should government support those who are digitally excluded?

Answer: Yes

The government should legislate that traditional identity routes remain available. Paper and physical identity should not be slowly withdrawn because the digital system is cheaper or more convenient for departments.

People should have a right to opt out and a right to equivalent access. The system should be designed so that refusal to use digital ID does not create a lower class of citizen.

Human rights and civil liberties are more important than administrative convenience. Digital devices must never become a mandatory requirement for daily living. A person should be able to work, rent, access healthcare, access public services, travel domestically, use money and participate in ordinary life without being forced into a digital identity system.

The government should also guard against “soft compulsion”. If digital routes become faster, cheaper, easier or more respected than non-digital routes, the digital ID becomes mandatory in practice. That would undermine trust.

Chapter 4.4: Accessibility

4.4.Q1. Which organisations should the government engage with?

The government should engage civil liberties, privacy, disability, children’s rights, digital inclusion, cybersecurity, open-source and technical standards organisations. Examples include the Electronic Frontier Foundation, Open Rights Group, Privacy International, Big Brother Watch, the Information Commissioner’s Office, the National Cyber Security Centre, the Ada Lovelace Institute, children’s charities, disability rights organisations, digital inclusion charities, W3C, the OpenID Foundation and the Decentralized Identity Foundation.

The government should also engage open-source technologists and decentralised identity experts who are not tied to large procurement vendors.

Chapter 4.5: Alternative access routes

4.5.Q1. What are the most important barriers to address when designing alternative access routes?

The most important barrier is ensuring that alternatives are real, not symbolic. If non-digital routes are slow, expensive, inconvenient or treated as inferior, the digital ID becomes mandatory in practice. Alternative routes should protect privacy, support people without devices, support people with disabilities, support people in crisis and provide resilience when digital systems fail.

The government should also prevent penalty pricing. It would be unethical if people who choose not to use digital ID are pushed into more expensive, slower or less convenient routes simply to pressure adoption. Alternative access should be affordable, dignified and functionally equivalent wherever possible.

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

A passport, physical documents, assisted human support and a legally protected route to access services without a smartphone.

Alternative routes should include familiar, human and physical methods of proving identity. Paper documents, secure cards, passports with chip-based technology, assisted verification and face-to-face support may all have a role. The key principle is that the person should not be penalised for choosing an analogue or non-smartphone route.

The government should not raise costs, reduce service quality or create administrative friction in order to push people into digital identity. That would be coercive by design, even if the digital ID remained technically optional.

Revised Part 5: Trusted

Chapter 5.1: Data protection and privacy

5.1.Q1. Are there additional measures to further protect user data?

Answer: Yes

Additional measures should include strong data minimisation, user-visible access logs, independent audits, open technical standards, public threat modelling, external cryptographic review, privacy impact assessments, biometric impact assessments, strict retention limits, purpose limitation, sector-specific or pairwise identifiers, and meaningful penalties for misuse.

The system should avoid unnecessary centralisation. Sensitive data should not be copied or pooled merely because it is technically convenient. The more data that is centralised, the greater the cybersecurity, national security and civil liberties risk.

Government-issued credentials should also be portable into certified, privacy-preserving and citizen-controlled systems beyond the GOV.UK Wallet. Citizens should not be forced to use a single

government-branded app as the only practical route to digital proof. If the credential is genuinely theirs to hold and use, it should be capable of supporting wider trusted systems, including decentralised and self-sovereign identity approaches, without making government the centre of every transaction. Government should support self-sovereign and decentralised identity research, including approaches that allow government-issued credentials to strengthen citizen-controlled proofs without making government the centre of every transaction.

5.1.Q2. How should government ensure transparency around how national digital ID data is used?

Transparency should be practical, not just policy-based. Citizens should be able to see when their credential has been used, what was shared, who requested it, for what stated purpose and how long any record is retained.

Every access, lookup, credential use, status check, revocation event or data-sharing event should create a user-visible record wherever possible. Citizens should have a clear breadcrumb trail showing how their digital ID has been used. Transparency should not depend on submitting a subject access request after harm has already occurred. It should be built into the user experience.

There should be a public register of authorised checkers, wallet providers, data-sharing gateways, legal gateways, processors and subcontractors. There should also be transparency reports showing usage volumes, revocations, appeals, errors, complaints, breaches, law enforcement requests and private-sector adoption.

The most powerful transparency measure would be architectural: reduce the need for government involvement in daily verification. If most everyday proofs are performed locally and selectively, there is less hidden data use to explain and less trust to ask citizens to grant blindly.

Chapter 5.2: Securing the national digital ID system

5.2.Q1. Are there additional security safeguards that should be considered?

Answer: Yes

Additional safeguards should include post-quantum readiness, crypto-agility, independent penetration testing, open cryptographic review, hardware-backed credentials, secure recovery, anti-coercion design, device loss recovery, phishing-resistant authentication, insider-threat controls, supply-chain security, vendor exit plans and resilience against cloud provider compromise.

The system should be designed for the world we are entering, not the world we are leaving. AI-enabled fraud, deepfakes, synthetic documents, automated social engineering and agentic systems will make identity attacks faster and more convincing. The architecture should assume that identity fraud will become more automated, more scalable and more difficult for humans to detect.

Security planning should also consider highly capable future automated systems. A national digital identity system must be protected not only against today's attackers, but against future environments where automated systems can discover vulnerabilities, impersonate humans, generate convincing fraud attempts and attack infrastructure at a scale beyond normal human capability.

This is one reason the root of trust should not be concentrated in one institution, one database, one vendor, one cloud provider or one checker model. A decentralised, user-controlled trust architecture makes systemic capture harder. It should not be possible for an attacker, rogue insider, compromised vendor or automated system to compromise the trust layer by breaching one central point.

Security should not rely only on stronger central systems. It should also reduce the amount of data exposed, reduce the number of times sensitive data is shared, and design out unnecessary single points of failure.

Chapter 5.3: Fraud as a national challenge

5.3.Q1. What are the most important factors in ensuring alternative access routes are secure?

Alternative access routes must be secure without becoming inaccessible. Key factors include trained staff, strong identity proofing, fraud-resistant recovery, safeguards against coercion, clear escalation routes, auditability, rate limits, manual review for complex cases and clear routes for correction.

The system should not create weak recovery channels that attackers can exploit. At the same time, it must not lock out genuine users who have lost a device or lack documents. This balance is crucial. The government should also recognise that fraud cannot be solved by government digital ID alone. The internet now faces a wider trust problem involving synthetic identities, automated accounts, deepfakes, fake documents, impersonation, compromised devices and AI-assisted fraud.

A privacy-preserving, zero-knowledge and Sybil-resistant identity layer could add resilience by helping people and services prove uniqueness, validity or eligibility without exposing unnecessary personal data. This is where public-good decentralised identity infrastructure could support, rather than replace, government credentials.

A government credential may provide a strong official fact, while a decentralised proof layer can help preserve privacy, reduce dependency on government lookups and strengthen trust across the wider internet.

5.3.Q2. What factors are important in ensuring alternative access routes are not misused by fraudulent actors?

Alternative routes should use proportionate risk-based checks, not blanket surveillance. They should be monitored for abuse, but safeguards must not punish vulnerable people for having complex circumstances.

Fraud prevention should focus on strong proofing, secure recovery, staff training, tamper-evident audit trails and minimal data exposure. A decentralised proof-of-personhood or trust-anchor layer could add resilience in future by making it harder for synthetic identities and repeat fraudsters to operate, while still protecting privacy for genuine users.

The government should not try to solve the entire trust problem through a single state identity layer. That would increase dependency on government infrastructure and may reduce public trust. A better model is layered: government credentials for official facts, decentralised public-good trust infrastructure for privacy-preserving proofs, and strict limits on what businesses or departments can request.

Chapter 5.4: Ensuring strong oversight and governance

5.4.Q1. What additional oversight mechanisms should be put in place?

There should be independent statutory oversight with real powers. Oversight should include Parliament, the Information Commissioner, cybersecurity experts, civil society, disability and inclusion representatives, children's rights experts and independent technologists.

There should be mandatory public reporting, independent audits, privacy impact assessments, biometric audits, human rights impact assessments and a clear prohibition on function creep without fresh legislation and scrutiny.

The government should also create an independent technical advisory board with open-source, decentralised identity, cryptography, cybersecurity and civil liberties expertise. This should not be dominated by vendors who may benefit commercially from the system.

Open-source scrutiny should be a core governance principle wherever possible. The public does not need vague assurances that the system is safe. It needs inspectable standards, transparent legal frameworks, independent technical review, published threat models, clear accountability and visible safeguards for people who are hesitant, excluded or opposed to digital ID.

5.4.Q2. What measures could help people resolve issues with their national digital ID?

People need rapid human support, not only automated helpdesks. AI support may be useful for triage and guidance, but identity errors can affect work, money, housing and essential services. There must be accountable human review.

There should be clear service standards, emergency unlock routes, appeal rights, compensation where harm is caused, accessible complaint routes and an independent ombudsman-style escalation route. A person should never be trapped inside an automated identity failure loop. If the system blocks a person from work, housing, benefits, healthcare, banking or essential services, there must be a rapid route to human intervention with authority to correct the issue.

5.4.Q3. What additional oversight mechanisms would help you trust the national digital ID system?

I would trust the system more if the government clearly committed that the national digital ID will not be the centre of daily identity verification. It should be one credential within a broader, open, privacy-preserving ecosystem.

Trust would also be improved by a legal right to alternatives, a ban on mandatory private-sector use, independent oversight, user-visible logs, no general-purpose private-sector identifier, no routine call-home verification and open technical standards.

The system should also be subject to public scrutiny from the beginning. That includes open standards, published governance rules, clear legal limits, transparent procurement, independent technical challenge and meaningful engagement with civil society, privacy groups and public-good technologists.

5.4.Q4. What measures should be in place to help you feel confident resolving issues?

There should be clear accountability, rapid correction, human review, independent appeal, urgent service access where the digital ID fails and a permanent non-digital fallback.

I would also welcome meaningful engagement with innovators, civil society and open-source public-good projects working on privacy-preserving identity, including .zkdid™. This consultation should not only hear from large incumbent vendors or departments that already favour centralised infrastructure.

The government should show that it is willing to learn from decentralised, open-source and privacy-preserving identity research. Public trust is unlikely to be won by closed procurement, opaque technical choices or reassurance alone. It will be won by restraint, transparency, open scrutiny, enforceable rights and architecture that gives citizens real control.

Part 6: Wider summary of impacts

6.1.Q1. Are there other benefits for businesses from introducing the national digital ID system?

Answer: Yes

Potential benefits include reduced fraud, lower document-handling risk, faster onboarding, fewer stored copies of passports and driving licences, easier age checks, more reliable right-to-work checks and reduced compliance friction.

If designed well, the system could also help foster a new UK digital trust industry built around privacy, security, user control, selective disclosure and citizen sovereignty over personal data. Businesses could

benefit from safer verification without needing to collect, store or monetise excessive personal information.

These benefits depend on the system being trusted. If citizens resist it, or if businesses fear liability, integration cost or reputational risk, adoption may be slower than expected.

6.1.Q2. Are there other costs to businesses from introducing the national digital ID system?

Answer: Yes

Costs include staff training, software integration, hardware or terminal upgrades, compliance processes, cyber insurance, support for customers without digital ID, accessibility adjustments, liability management and dependency on third-party providers.

Small businesses may be disproportionately affected if digital checking becomes mandatory or expected across many use cases.

Government should not simply push the cost of a major national policy shift onto businesses and expect them to absorb it. If businesses are expected to integrate with digital ID systems, especially small businesses, there should be clear guidance, simple tools, proportionate compliance requirements, support for implementation and protection from unfair liability.

The government should also avoid creating another complex digital compliance burden that businesses feel they have no practical choice but to accept. Public trust will be weakened if digital ID is experienced as an unfunded mandate imposed on citizens and businesses alike.

6.1.Q3. Are there other benefits for households from introducing the national digital ID system?

Answer: Yes, if implemented with safeguards

Households could benefit from less paperwork, faster access to services, reduced over-disclosure of personal information and better protection against identity fraud.

Households could also benefit from a future where personal data is more secure, more portable and more under the individual's control. A well-designed system could help citizens prove facts without constantly handing over copies of documents, addresses, dates of birth or other sensitive information. However, these benefits depend on privacy, trust and alternatives. A household does not benefit if the digital ID becomes another compulsory system to manage, another point of failure, or another way to be excluded.

6.1.Q4. Are there other costs to households from introducing the national digital ID system?

Answer: Yes

Although the system may be free at the point of use, it is not free in reality. It will be funded by taxpayers and will require devices, connectivity, support, recovery processes, training and ongoing infrastructure.

Households may also face indirect costs: needing newer phones, losing time dealing with technical failures, needing support for elderly relatives, or being forced into digital channels they do not trust or understand.

There is also a democratic cost if people feel they are paying for a system they did not want, cannot easily refuse and must still fund through taxation. That makes genuine opt-out rights, physical alternatives and transparent cost assessment essential.

Done well, the long-term savings from fraud reduction and better public services may outweigh these costs. Done badly, it could become an expensive centralised infrastructure project that damages public trust.

6.1.Q5. Are there other wider impacts from introducing the national digital ID system?**Answer: Yes**

The wider impact is trust in democracy itself. Digital ID is not a normal IT project. It changes the relationship between citizen, state and private sector. If the public believes the system is being forced in through the back door, trust will collapse.

The UK has an opportunity to lead in a better direction: privacy-preserving, open, interoperable, decentralised where possible, citizen-controlled and resistant to capture. This would strengthen public services while protecting civil liberties.

The government should therefore treat digital ID as public infrastructure that must be earned, not imposed. Trust is the whole system. Without trust, even technically strong digital identity will fail.

The trust paradox is real. The more powerful the digital identity system becomes, the more important it is that people believe it cannot be misused. Public distrust does not require every citizen to understand the technology in detail. If people sense that the system is becoming a tool of monitoring, exclusion or control, resistance will grow regardless of the technical safeguards.

Handled properly, digital ID could contribute to a safer society, a safer internet, reduced cybercrime, better access to public services and renewed trust in democratic institutions. Handled badly, it could produce the opposite: public resistance, reduced trust in government, legal challenge, private-sector overreach and long-term damage to democratic legitimacy.

Closing Statement

The national digital ID system could improve public services, reduce fraud and reduce unnecessary document sharing. I support those aims. However, the same infrastructure could also create serious risks if it becomes a universal permissioning layer across employment, public services, private-sector transactions and online life.

The government should therefore commit to a narrow, privacy-preserving, optional and independently governed model. It should avoid a single universal identifier, avoid routine call-home verification, preserve physical alternatives, support open standards and ensure that government credentials do not become the root of digital personhood.

The strongest path is not to force trust. It is to earn trust by empowering citizens. A government-issued digital credential can be valuable, but it should support a broader sovereign identity ecosystem rather than replace it.

This is a moment where the government must be honest with itself. Digital identity can either rebuild trust or destroy it. It can help create a safer internet, reduce fraud, protect citizens and strengthen democracy. Or, if designed carelessly, it can deepen distrust, increase dependency, enable overreach and make people feel that access to ordinary life is being mediated by the state.

The right compromise is clear: use government digital ID as a trusted source of official facts, but do not make it the root of personhood. Build with privacy, openness, decentralisation, human rights, non-digital alternatives and citizen control at the centre. That is how the UK can move towards digital trust without sacrificing democratic trust.