coinbase

To:
Rt Hon Darren Jones
House of Commons
London
SW1A 0AA

c/o Digital ID
Cabinet Office, 70 Whitehall, London, SW1A 2AS, United Kingdom

05 May 2026

Re: Consultation on "Making public services work for you with your digital identity"

Coinbase Global, Inc. (together with its UK subsidiaries, "**Coinbase**") appreciates the opportunity to respond to the Cabinet Office's consultation on the proposed national digital identity system for the United Kingdom.

Coinbase was founded in 2012 with the idea that anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, we are publicly listed in the United States and provide a trusted and easy-to-use platform that millions of verified users in over 100 countries rely on to access the crypto economy.

Coinbase supports the Government's commitment to building a digital ID system that is useful, inclusive and trusted, and that the digital ID will be voluntary with design decisions informed by public engagement.

We write to offer perspectives on how the Government can deliver on its stated principles and overcome public concerns, particularly on privacy, user control and security, by ensuring that decentralised identity (DID) technologies are explicitly accommodated within the UK Digital Identity and Attributes Trust Framework and the wider digital ID ecosystem. We believe a technology-neutral framework that creates a level playing field for both centralised and decentralised approaches will produce a stronger, more resilient and more trustworthy system for the United Kingdom.

We offer detailed comments below and look forward to continuing to work with the Government on these important issues.

Yours sincerely,

Katie Harries, Head of Europe Policy

Introduction

The Government has set out that it believes the current patchwork of identity documents, including passports, driving licences and utility bills, is burdensome, exclusionary and insecure, and that it wants a modern means of proving identity digitally, supported by core design principles of usefulness, inclusivity and trust.

While the potential benefits are easy to recognise, there are also strong concerns with the national digital ID proposals. Critics have warned that the scheme risks creating centralised repositories of sensitive personal data, concentrating control over identity in a single government system, and expanding the potential for surveillance.

This concern is based on how the consultation describes a system built primarily on GOV.UK One Login and the GOV.UK Wallet, with the possibility that third-party wallets may hold the digital ID if they meet certification standards. However, the framework as currently described appears to assume a particular architecture — one in which the government issues a verifiable credential, the user stores it in a certified wallet, and verification is mediated by certified digital verification service (DVS) providers.

There is a better approach. The government should focus potential solutions on Decentralised Identity (DID), which address these concerns through identity management in which individuals, rather than central authorities or major platforms, hold and control their own verified credentials. Enabled by cryptographic proofs and, in many implementations, decentralised ledgers, DID delivers increased privacy, portability and security while reducing dependence on large, centralised data stores.

DID is not merely a theoretical proposition.

- Estonia pioneered blockchain-enabled decentralised identity over two decades ago, achieving nearly 99 per cent blockchain-based digital ID adoption among its citizens.
- Singapore's SingPass provides a decentralised login solution used across public and private sector services.
- In the United States, California has begun testing a mobile driver's licence application built with decentralised identity technology.

We urge the Government to adopt a technology-neutral approach that explicitly includes decentralised identity as a permissible architecture within the UK Digital Identity and Attributes Trust Framework. The Trust Framework already sets out standards for privacy, security and inclusivity; those standards should be met by any qualifying technology, whether centralised or decentralised, without the framework privileging one architectural model over another.

Pursuing a technology neutral approach that permits DID within this framework would:

- **Deliver on the Government's own privacy commitments.** The consultation emphasises data minimisation, selective disclosure and user control. DID achieves these by design: credentials are held in the user's own wallet, shared only with their explicit consent, and verified cryptographically without requiring a centralised intermediary to broker the exchange.
- **Reduce systemic security risk.** Centralised databases of identity data are high-value targets for attackers or "honey pots." DID eliminates the need for such repositories, because each credential is user-held and verified against cryptographic proofs rather than a central store.
- **Build public trust.** By demonstrating that the system is architecturally open and that no single technology provider or government department holds a monopoly over how citizens prove their identity, the Government can address civil-liberties concerns more convincingly than any privacy notice alone.

The government must not allow the framework to lock in a single architecture risks obsolescence. A technology-neutral standard allows the ecosystem to incorporate advances, including zero-knowledge proofs, verifiable credentials on public blockchains and other innovations, as they mature.

We set out our detailed positions below, first addressing key themes and then responding to specific consultation questions.

Thematic response: Decentralised identity and the UK Trust Framework

Technology neutrality as a design principle

Decentralised identity allows credentials to be issued by any trusted party (including government), stored in any standards-compliant wallet, and verified by any relying party through cryptographic proof — potentially without the need for an intermediary DVS to broker the transaction. Such an approach would dominate a solution that locks in a verification process that requires centralised DVS providers.

Such an approach is also consistent with the drafting of Trust Framework, which is written in terms of outcomes (security, privacy, accuracy, non-repudiation) rather than prescribing specific technical plumbing. This ensures that providers using different architectures can compete on merit, and that users benefit from the resulting innovation.

A practical point on certification follows from this. The consultation envisages that third-party providers will be "independently certified" under the Trust Framework — a model that assumes a corporate entity sitting behind a service. Decentralised services do not always fit that model, but this is not a barrier to certification. The transparency and external verifiability of well-designed smart contracts is itself a form of independent

certification: the code is open and inspectable, behaviour is determined by the protocol rather than an operator's discretion, and any third party can audit and formally verify how the system works. The Framework should evolve to recognise this alongside the existing entity-based certification model.

A related point concerns the regulatory model under the Data (Use and Access) Act 2025. The DVS regime was designed around the assumption of a centralised service provider that holds, processes or transmits user data on behalf of others. Decentralised wallets and smart-contract-based credential systems, by design, retain data with the end user and do not place a centralised intermediary in the data path. Applying DVS-style requirements wholesale to such systems would, in some cases, be conceptually mismatched and operationally counter-productive. The outcomes the regime targets, including user protection, fraud prevention and accountability, should be achieved through requirements appropriate to the architecture, rather than by transposing rules built for centralised intermediaries.

Addressing privacy and civil-liberties concerns

The consultation acknowledges that the digital ID will contain sensitive information such as full name, date of birth, nationality and a biometric facial image and that privacy is a central concern. The Government's commitment to selective disclosure and data minimisation is commendable. However, DID goes further in several important respects:

Concern	Centralised approach	Decentralised approach
Data Storage	Identity data held in government or provider databases	Each credential is user-held; no central repository
Consent	Mediated by platform design; can be opaque	Explicit, auditable consent via the user's own wallet
Trust model	Requires faith in central authorities	Trust is distributed and cryptographically verifiable
Breach risk	Large databases create high-value targets	No centralised "honey pot" to attack
Interoperability	Risk of walled gardens	Portable and interoperable by default

It is worth addressing a common misconception that arises in public debate. "Decentralised" or "blockchain-based" identity does not mean that personal data is shared with everyone on a network. Properly designed decentralised systems make the rules of credential issuance and verification transparent, so that anyone can audit how the system works, while keeping the personal data itself private to the user and the parties they explicitly authorise. Programmable smart contracts can support automated and obfuscated credential exchange in which the only thing the rest of the network sees is a

cryptographic confirmation that a valid proof was produced. Transparency of mechanism and confidentiality of personal data are complementary properties, not opposites.

By accommodating DID within the Trust Framework, the Government can offer citizens a choice: those who are comfortable with the GOV.UK Wallet can use it; those who prefer a decentralised, self-sovereign approach can use a certified DID-based wallet instead. This optionality is itself both a privacy-enhancing measure and a resilience-enhancing one. It prevents any single system from becoming a mandatory chokepoint, distributes the risk of outages or compromise across multiple wallets, and gives users meaningful choice, particularly those whose needs are not well served by a single government-operated app. Maximising the number of robust, certified routes to managing and verifying the national digital ID is good for privacy, good for inclusion, and good for system resilience.

Institutional and economic benefits

DID also offers significant benefits to relying parties: the businesses, public services and other organisations that need to check identity. Under a DID model, relying parties verify credentials cryptographically rather than by accessing a centralised database or storing copies of sensitive documents. This reduces their data-protection compliance burden, lowers their exposure to data-breach liability and can significantly reduce the time and cost of onboarding and identity checks. These benefits are particularly relevant to the Government's ambition to make right-to-work checks fully digital and to reduce fraud across the economy.

Conclusion

Our core recommendation is straightforward: the UK Digital Identity and Attributes Trust Framework should be technology-neutral and should explicitly accommodate decentralised identity as a permissible architecture alongside the proposed GOV.UK Wallet model. This is not an abstract ideological position; it is the practical means by which the Government can deliver on its own stated commitments to privacy, user control, security, and innovation.

Decentralised identity eliminates centralised data repositories that attract cyber attack. It gives users genuine, structural control over their credentials rather than relying on platform design choices to mediate that control. It reduces compliance burdens for relying parties. And it creates a competitive, innovative ecosystem in which the best technologies can earn public trust on merit.

The Government has an opportunity to embrace modern technology while safeguarding civil liberties. We encourage the Government to seize that opportunity, and we stand ready to support this work including participation in pilots, technical working groups, and further consultations as the framework develops.

Responses to specific consultation questions

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

Any benefits the Government foresees will only be achieved if the system is architecturally open. A framework that accommodates multiple technology approaches including decentralised identity will produce a more resilient, innovative and privacy-preserving ecosystem than one built around a single centralised model. The Government should ensure that the UK Digital Identity and Attributes Trust Framework is technology-neutral and that certification standards are expressed in terms of outcomes rather than prescribed architectures.

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

The most significant risk is that the system, if designed around a single centralised architecture, could create large repositories of sensitive personal data that become attractive targets for cyber attack and potential vectors for surveillance. Public trust will be difficult to build and easy to lose; a single high-profile breach or misuse incident could undermine adoption for years.

A second risk is technological lock-in. If the framework is written around the specific capabilities of the GOV.UK Wallet and current DVS infrastructure, it may be difficult to incorporate superior technologies as they emerge. Decentralised identity, zero-knowledge proofs and other privacy-enhancing technologies are advancing rapidly; the framework must be flexible enough to absorb them.

A third risk is that mandatory digital right-to-work checks, coupled with a narrow range of accepted evidence, could create exclusion for individuals who face barriers to accessing the digital ID — particularly if alternative access routes are insufficiently robust. We address this further in our response to Part 3 questions.

Finally, the Government should guard against the risk that a Government Checker service, if offered at low or no cost, could crowd out private-sector innovation in the digital verification market. A level playing field between government and private-sector services is essential to maintaining a competitive, innovative ecosystem.

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

Yes, strongly. User choice in wallet provision is essential — both for practical reasons and for the credibility of the Government's commitment to privacy and user control. If the

digital ID can only be held in the GOV.UK Wallet, the system becomes a single point of failure and a single point of control. Allowing certified third-party wallets, including decentralised wallets, to hold the digital ID:

- gives users meaningful choice over how their identity data is stored and managed;
- creates competitive pressure that drives improvements in security, usability and privacy;
- reduces systemic risk by distributing credentials across multiple wallet providers rather than concentrating them in a single government application;
- supports the Government's stated principle that the digital ID is voluntary — a principle that is more credible when users also have a choice of how to hold it.

The certification requirements for third-party wallets should be rigorous, outcome-based and technology-neutral. They should address security, data protection, revocation handling and user authentication, but should not prescribe a particular technical architecture. A decentralised wallet that meets these standards should be certified on the same terms as a centralised one.

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

The proposal to create a universal unique identifier tied to the digital ID raises significant technical challenges:

- **Privacy-preserving matching.** If a single identifier is used across all public services, it becomes a powerful correlation tool. Decentralised identity offers an alternative: sector-specific or context-specific identifiers derived from a root identity, which allow matching within a defined scope (e.g., health services) without enabling cross-sector correlation by default. This approach is more consistent with data-minimisation principles.
- **Revocability and unlinkability.** If a universal identifier is compromised, the individual's interactions across all services are exposed. The system should be designed so that identifiers can be rotated or revoked without disrupting service access.
- **Consent architecture.** Cross-service matching should be subject to granular, revocable user consent. Users should be able to see which services hold their identifier and withdraw consent for specific linkages.
- **Interoperability with decentralised credentials.** The matching mechanism should work with credentials held in any certified wallet, not only the GOV.UK Wallet. If matching relies on data held within a specific wallet's infrastructure, it creates an architectural dependency that undermines technology neutrality.

We recommend that the Government explore privacy-enhancing technologies, including zero-knowledge proofs and pairwise identifiers, as part of the technical design for cross-service matching. These technologies allow verification of facts about a person (e.g., "this is the same individual who accessed Service A") without revealing the underlying identifier to the verifier.

3.3.Q1. To what extent do you agree or disagree that the private sector and third parties should be able to use the digital ID alongside other options?

We strongly agree. The digital ID should be one option among several for proving identity in the private sector, not the only option or the default. This is important for three reasons:

First, it preserves genuine voluntariness. If the digital ID becomes the only practically available proof of identity — because physical documents are progressively de-recognised or because relying parties find it cheaper to accept only digital checks — then the system is mandatory in all but name.

Second, it maintains a competitive market for identity verification. Private-sector DVS providers, including those offering decentralised identity solutions, should be able to compete with the digital ID on security, privacy and user experience. This competition benefits users.

Third, it supports inclusion. Some individuals will, for legitimate reasons, prefer not to use a government-issued digital ID. They should not be disadvantaged in their ability to access goods and services.

We also note that the phrase "other appropriate digital identities from third parties" in the question wording is important. The Trust Framework should certify decentralised identity credentials, issued by trusted parties and held in certified wallets, as "appropriate digital identities" on the same terms as the national digital ID. This is the practical meaning of technology neutrality.

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

Transparency is essential to public trust, and the Government should go beyond standard privacy notices. We recommend:

- **A public, machine-readable register of data-sharing arrangements** between government departments and with any third-party services that interact with the digital ID system. This register should specify what data is shared, with whom, for what purposes, and under what legal basis.
- **User-facing audit logs** that allow individuals to see, in real time, which organisations have verified their digital ID, what information was disclosed, and

when. This is a natural feature of decentralised identity systems, where the user's wallet records every presentation event. The GOV.UK Wallet should offer equivalent functionality.

- **Annual transparency reports** on the operation of the digital ID system, including aggregate statistics on usage, data-sharing, revocations, complaints, and any law-enforcement access requests — published by the responsible department and laid before Parliament.
- **Open-source publication of core components** of the digital ID system's code, to enable independent security review and build confidence in the system's integrity.

Decentralised identity architectures offer a structural advantage here: because the user mediates every data exchange, transparency is built in rather than bolted on. The Government should consider this architectural benefit when evaluating technology options.

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

Yes. Beyond the cyber-security standards referenced in the consultation (Cyber Assessment Framework and Secure by Design), we recommend:

- **Elimination of centralised "honey pots."** The system should be designed to minimise the aggregation of identity data in any single repository. Decentralised identity achieves this structurally: because credentials are user-held and verified cryptographically, there is no central database of all citizens' identity data to be breached. Even if the GOV.UK Wallet remains the primary storage mechanism, the back-end architecture should avoid creating a single, consolidated identity database.
- **Hardware-backed credential storage.** Where devices support it, credentials should be stored in a hardware-secure element (e.g., a device's Trusted Execution Environment or Secure Enclave), making them resistant to extraction even if the device is compromised.
- **Regular independent penetration testing and red-team exercises**, with results summarised in the annual transparency report.
- **Incident-response and breach-notification commitments** that go beyond the minimum requirements of the UK GDPR, given the sensitivity and scale of the data involved.
- **Resilience to quantum computing threats.** The cryptographic foundations of the digital ID — particularly any blockchain-based components — should be designed or upgradeable to resist quantum attacks, in line with NCSC guidance on post-quantum cryptography.