Open consultation: Making public services work for you with your digital identity

Comms Council UK (CCUK) response

Consultation title	Making public services work for you with your digital identity
Full name	Ana Thompson Perea
Representing (individual/organisation)	Organisation
Organisation name	Comms Council UK (CCUK)
Email address	team@commscouncil.uk

About CCUK

1. Comms Council UK is a membership-led organisation that both represents and supports telecommunications companies that provide services to business and residential customers in the UK. We keep Britain talking in its various guises by providing or reselling voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video.

2. The membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly. CCUK represents its members at a policy level, builds coalitions to collaborate on industry initiatives and provides a platform to help members prepare for change, learn about new trends and develop new business relationships.

3. CCUK welcomes the opportunity to respond to this Consultation. Our response is primarily covering Chapter 5 of the Consultation: *Trusted,* and Chapter 5.3 in particular: *Fraud as a national challenge*.

General Comments

4. CCUK supports the Government's proposals for a national digital ID in principle, recognising the significant potential to prevent and tackle fraud across the economy and to streamline robust Know Your Customer (KYC) and right to work checks.

5. In particular, CCUK welcomes the Government's recognition in this consultation that fraud – and particularly identity misuse – is a national security, economic and consumer protection challenge, and that the national digital ID will be a high-value target for scammers, organised crime and malicious actors. This aligns with CCUK's long-standing position that tackling fraud requires a proactive, whole-ecosystem approach that spans

telecoms, financial services, digital platforms and law enforcement, backed by effective enforcement against bad actors and stronger, modernised technical foundations (for example, around number management and identity assurance). The telecoms sector requires solutions that will enable the identification of bad actors within the sector, prevent these parties from continuing to operate and support the sharing of information that will enable other organisations such as Law Enforcement to be proactive.

6. We therefore strongly support the intent to design robust fraud-prevention measures into the digital ID system from the outset, and to integrate this work with the wider Fraud Strategy 2026 to 2029.

7. However, we consider that this can only be achieved safely if the system is underpinned by strong guardrails: clear liability and assurance frameworks for relying parties; strict data-minimisation and selective disclosure; robust standards around alternative access routes (which may be most attractive to fraudsters); and close alignment with existing KYC regimes and fraud controls in regulated sectors.

8. A critical design principle that must underpin the system is *contextual disclosure*: individuals should not be required to assert or verify their identity merely to access a digital service. Identity proofing should be triggered only at the point of genuine necessity. For example, at the point of a transaction, age verification, or contract formation, it may be necessary, but not as a condition of entry to or browsing across digital properties. A consumer visiting a website to compare prices, read content, or explore services should be able to do so without any identity credential being requested or inferred. This mirrors the principle established in UK GDPR Article 5(1)(b) (purpose limitation) and Article 25 (data protection by design), which together require that personal data, including identity authentication, are not collected beyond what is strictly necessary for the specific purpose at hand. The Government should make explicit in the framework that relying parties may not mandate identity checks as a blanket condition of service access, and that the digital ID infrastructure must be architected to prevent passive or ambient identity assertion. This is particularly important given Google's reliance on individuals' identity as a common match key for improving the ad monetization of its properties (e.g., Customer Match).

9. Our response therefore focuses on the conditions under which a national digital ID can enhance fraud prevention and consumer protection without creating new systemic vulnerabilities or shifting disproportionate risk and cost onto industry.

Responses to consultation questions

Part 1: Our Ambition

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

10. CCUK considers the main benefits to be: 1) Stronger prevention and detection of fraud and identity misuse, by providing a higher-assurance, verifiable credential that can be checked in real time; 2) More consistent and efficient KYC / onboarding across sectors, enabling organisations to rely on a common, trusted credential rather than duplicating

complex identity checks; 3) Improved protection for consumers and businesses through reduced account takeover, fewer opportunities for impersonation, and better audit trails when fraud does occur; and 4) Support for law enforcement and regulatory activity, when appropriately governed, by improving the quality and reliability of identity data used to investigate fraud and related crime.

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

11. Potential drawbacks include: 1) Concentration of risk if not properly secured and governed, as a single foundational ID could become a high-value target for attackers, with significant systemic consequences if compromised; 2) Risk of over-reliance by relying parties, as some organisations may treat a valid digital ID as sufficient on its own, even in higher-risk scenarios where additional checks are still necessary; and 3) Differences in how sectors integrate and use the digital ID could create gaps or inconsistencies that fraudsters exploit.

1.0.Q3. One of the government's aims for the new national digital ID system is to make it easier for people to prove who they are. To what extent do you agree or disagree that the proposed system could help achieve this aim, and why?

Somewhat agree

1.0.Q3.1. Please explain your answer

12. In principle, a reusable, high-assurance digital ID should make it much easier and faster for people to prove who they are, particularly in repeated interactions across different services. However, effectiveness depends on high uptake and broad acceptance across key sectors (finance, utilities, telecoms, employment); strong inclusion and support measures so people without high-end devices or digital confidence can still participate; and clear technical and assurance standards, so relying parties understand what level of proof they are actually receiving and when they should layer on additional checks.

1.0. Q.4 .The government proposes to use the digital ID system to enable more modern, efficient and personalised public services. Which public services would you want the government to prioritise making faster or more efficient using the system?

13. From a fraud-prevention and KYC perspective, CCUK would prioritise areas that combine high fraud risk, high transaction volumes and material impacts on individuals and the public finances.

Part 3: Useful

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

Strongly Agree

3.3.Q1.1.Please explain your answer

14. Allowing regulated private-sector organisations and third parties to use the digital ID alongside existing options will improve fraud prevention and KYC by providing a higher-assurance alternative to paper-based checks; reduce friction for consumers who often have to repeat similar identity processes with multiple providers and encourage standardisation of basic identity assurance across sectors. However all relying parties must comply with robust data protection, security and fraud-control requirements.

15. CCUK draws the Government's attention to a significant competition risk arising from platform-level identity requirements that could distort how digital services are monetised. Where dominant platforms condition service access on verified identity, they create structural advantages for subscription-based business models at the expense of advertising-supported services that fund the majority of online services, particularly those operated by smaller, independent providers.

16. This asymmetry operates on two levels. First, under prevailing app store rules, developers who collect subscriptions via in-app mechanisms are required to pay a platform commission (typically 15–30%), effectively a tax on their subscription revenue that does not apply to advertising-funded services. Identity-gating that nudges consumers toward subscription models therefore transfers revenue from smaller, ad-supported competitors to platform operators. Second, and critically, advertising-based monetisation does not require, and should not require, individual-level identity. Digital advertising can operate effectively using common object identifiers (such as device identifiers or pseudonymous advertising IDs) that function at the level of a device or session, rather than being linked to a specific individual. Recent ICO guidance and EEA jurisprudence, including the Scania line of cases and SRB-related data governance rulings, supports the view that where a recipient organisation has implemented appropriate technical and organisational measures to prevent re-identification, pseudonymous object identifiers held by that recipient are properly characterised as non-personal data in their hands.

17. The Government should therefore ensure that: (a) the digital ID framework does not incentivise or require identity assertion for advertising-funded services; (b) guidance explicitly distinguishes between identity-level verification (required for transactions and regulated KYC) and device-level or session-level identifiers (sufficient for most advertising use cases); and (c) the framework is reviewed for compatibility with the CMA's ongoing work on platform competition, app store rules, and digital advertising markets, to ensure that the system does not inadvertently reinforce the market power of platforms whose commercial model depends on identity aggregation.

Part 5: Trusted

5.1.Q2. Principles of data minimisation and empowering users to ensure they have greater control over how much data they share when using their national digital ID at point of use will be central to the design and implementation of the digital ID system. How should the government ensure transparency around how national digital ID data is used?

18. CCUK suggests publishing clear, layered explanations (high-level and technical) of how digital ID data flows between issuing bodies, checkers and relying parties, including for

fraud-prevention purposes and regular public reporting and independent review of how data is being used in practice, including statistics on fraud-prevention outcomes, complaints and any misuse incidents.

19. Transparency obligations should also extend to the distinction between identity-verified interactions and anonymous or pseudonymous interactions. Consumers should be clearly informed, in plain language, when identity is genuinely required for a given purpose, and when it is not. Platforms and relying parties that seek identity credentials beyond what is functionally necessary should be required to explain and justify that requirement. The Government should further clarify that object identifiers used for non-transactional digital interactions (such as browsing, content consumption, and digital advertising) do not constitute identity data under the framework, and that the digital ID system should not be used as a vehicle to normalise pervasive identity disclosure across the web.

5.3.Q1. 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?

20. On behalf of CCUK, we are minded to support the development of alternative access routes, provided they meet a comparable level of assurance and fraud resilience to the standard digital route. From a fraud and KYC perspective, the most important factors are the following:

    a. Alternative routes should be designed to meet the same identity assurance level (or a clearly defined and disclosed one) as the standard app-based journey. Where the same level cannot be achieved, this should be explicitly signposted to relying parties, so they can calibrate their own risk-based controls accordingly.

    b. Alternative routes should incorporate in-person or supervised checks where risk is higher (e.g. complex cases, vulnerable individuals, overseas documents); systematic verification against authoritative data sources wherever possible and strong controls around intermediaries.

    c. Government should design journeys that use appropriate multi-factor authentication and are clearly understandable to users, so they can recognise when a process deviates from the official pattern.

    d. Alternative routes should have: clear procedures for rapid revocation and re-issuance when compromise is suspected; audit trails of all access, use and recovery events that can be shared (where lawful) with financial institutions and other high-risk relying parties; and proactive review of dormant or anomalous credentials to prevent long-term abuse.

    e. For KYC and anti-fraud purposes, it is essential that firms understand what reliance they can place on a digital ID obtained via an alternative route. Government should therefore provide assurance that risk-based KYC and enhanced due diligence can still be applied where firms deem this necessary, even if a valid digital ID is presented.

f. The Government should confirm that alternative access routes, and the digital ID system generally, operate on a principle of proportionality of disclosure. Identity verification requirements must be calibrated to the specific risk and legal obligation involved. Browsing and price comparison activities carry no KYC obligation and should not be swept into identity-verification frameworks. The system should be designed so that the lowest level of assurance required for a given interaction is the maximum that can be demanded, and that relying parties are explicitly prohibited from requiring higher-assurance identity checks than the transaction warrants. This is consistent with the ICO's existing guidance on data minimisation and with the principle, recognised in competition law, that compulsory data collection beyond operational necessity may constitute an abuse of a dominant position (see Google Shopping, Case AT.39740, and the CMA's Mobile Ecosystems market study, 2022).

5.3.Q2. What do you think are the most important factors to consider when ensuring alternative access routes to the national digital ID are not misused by fraudulent actors?

21. From a fraud and KYC standpoint, the design of alternative access routes will be critical. We would highlight the following priorities:

    a. Tight control and supervision of intermediaries and assisted services: to prevent abuse, only vetted and accredited organisations should be permitted to provide assisted access and there should be clear operating standards, including identity checks on staff, training, and record-keeping.

    b. Minimising the data exposed through alternative routes: alternative access mechanisms should not expose full identity datasets that can be harvested for synthetic ID or impersonation and, where possible, should expose only the minimum attributes required for the specific transaction.

    c. Monitoring for unusual patterns in applications and flagging of suspicious access patterns, including mechanisms to share high-risk signals, where lawful, with other parties.

    d. Clear integration with existing frameworks: Government should make clear that the digital ID is a tool within a risk-based framework, not a mechanism that removes the need for further KYC checks where risk indicators exist. Guidance should explicitly align with existing KYC standards and supervisory expectations, so that regulated firms can incorporate the digital ID without weakening their controls. There should also be clarity on how firms should respond when a digital ID appears compromised, including routes to verification, revocation and remediation.

    e. Ongoing evaluation: As fraud threats evolve, the risk profile of alternative routes will also change. We would therefore encourage continuous engagement with high-risk relying parties to share intelligence and regular review of whether particular alternative routes are being disproportionately targeted.

22. These measures would help ensure that alternative access routes expand inclusion without creating new systemic fraud vulnerabilities or undermining existing KYC and financial crime controls.