GOV.UK

Consultation outcome

Digital Identity: Call for Evidence Response

Updated 8 September 2020

Contents

1. Introduction
2. Key issues raised
3. Analysis of responses received to each section
4. Next steps
5. Annex A – Digital Identity: Call for Evidence Questions, July 2019
6. Annex B – List of respondents

This publication is available at https://www.gov.uk/government/consultations/digital-identity/outcome/digital-identity-call-for-evidence-response

In these unprecedented times, government and businesses have needed to adapt quickly to provide online services, and change their processes. Being able to prove identity digitally has become essential to facilitate everyday tasks such as organising our finances.

In your responses to last year's digital identity Call for Evidence, you told us you wanted the government to take a lead role in developing the UK's digital identity economy. You wanted to see us create a clear framework that enables businesses to innovate. You wanted us to enable individuals to access the products and services they want with ease, confident that they are protected from fraud and that robust privacy protections are in place.

To this end we will develop proposals for a legal framework to remove regulatory barriers which prevent the use of secure digital identities and establish safeguards for citizens. We will also develop the next generation of digital identity use in government, and promote a pragmatic approach to international digital identity standards.

The foundation is strong. There is much that both the government and the private sector can continue to build upon to create trust in digital identities. We will work with individual users and business stakeholders, across departmental boundaries and with our international partners. This response to the call for evidence is just the beginning of an ongoing, and open, dialogue.

This government is committed to increasing online security, delivering personalised services, increasing productivity and boosting the economy. We will work at pace to realise this vision and look forward to working with you to support the next phase of the digital identity economy.

Matt Warman, Minister for Digital Infrastructure

Julia Lopez, Parliamentary Secretary for the Cabinet Office

1. Introduction

This is the government's analysis of responses to the Call for Evidence on digital identity. It forms part of an ongoing consultation process around digital identity that builds on previous government activities and engagement. The government will use the evidence supplied to shape future work on digital identity.

1.1 Background to the Call for Evidence

The government is committed to enabling a digital identity system fit for the UK's growing digital economy. A Call for Evidence was launched to better understand the potential of digital identity to:

- unlock the digital economy
- improve citizen experience and access to services
- safeguard privacy
- combat fraud in the digital space

Potential benefit: House buying and selling process

At the moment, people who are buying or selling their homes are required to prove their identity

multiple times throughout the process, whether to their bank, conveyancer or estate agent. This is time-consuming, expensive and repetitive for people and businesses, often requiring face-to-face verification or postage of sensitive identity documents. Effective use of digital identities (and digital signatures) would help simplify a lengthy process and enable more - if not all - of what is acknowledged to be one of life's most stressful experiences to be moved online. The result would be reduced friction, cost and abandoned transactions.

1.2 What we asked

The Call for Evidence focused on four key thematic areas where we wanted further information and insight. Questions fell within the categories of:

- needs and problems
- criteria for trust
- role of government
- role of private sector

The Call for Evidence was structured in this way to encourage contributions to some or all of the areas. The list of questions in each category can be seen in Annex A.[1] To widen reach and enable more detailed conversations, the Department for Digital, Culture, Media and Sport and Government Digital Service held events with industry and civil society in Birmingham, London and Edinburgh. These proved popular, with all the London places booked in 24 hours. Event feedback is supporting the development of policy. The level of enthusiasm and engagement of those who participated in the events was high. The government will continue to engage with industry and civil society as our work continues.[2]

1.3 Scale of responses

The Call for Evidence received 148 responses. A small number were out of scope, but the list of organisations providing in scope submissions can be found in Annex B.[3] 20 submissions were from individuals. Technology, professional services and finance sectors were most represented in the submissions. This may reflect areas of the economy where manual identity checking is a significant process and where digital identity has greatest potential. The government believes other sectors, such as the voluntary sector, may stand to benefit from digital identity and is working to bring their viewpoint into future conversations. The government did not receive many responses from citizens not already engaged with the debate on digital identity. The government is committed to do more to widen the discussion on digital identity.

A number of responses submitted by civil society organisations focused on a citizen/user perspective. These responses included evidenced commentary on instances where digital identity systems increase the exclusion of vulnerable users. This underlined how important it is that the government thinks carefully about what inclusivity means for digital identity to avoid design flaws which have unforeseen, harmful impacts.

2. Key issues raised

Respondents raised important issues and provided evidence across their answers to the Call for

Evidence questions on the below topics. Government is using these to prioritise policy development.

2.1 User privacy

Respondents recognised the importance of privacy protections for trust. Respondents had different opinions on what privacy meant in the context of digital identity. Some respondents from civil society cautioned that any digital identity system must not force the sharing of personal data or exploit the user into sharing more personal data.

2.2 Complex delivery models

Respondents did not agree on the best delivery model but warned that a lack of government action could create overly complicated or fragmented markets. Respondents agreed that in any digital identity model the ability to check or use authoritative government data is essential to successfully establishing a digital identity. A civil society respondent supplied evidence that some vulnerable users are excluded by complicated digital systems and that they need simple processes with simple reuse. The respondent recognised that prioritising this may mean sacrificing privacy but felt inclusion was more important.

2.3 Common language

Several responses identified that there is not a clear definition for digital identity, and what is meant when it is used. Respondents raised the point that when ‘digital identity’ is used it can mean a single identity, multiple identities or describe a technical process, depending on the speaker’s intent. Respondents argue this can cause confusion. Others wanted the government, civil society and industry to work together to increase the education level of the general public around digital identity so that it is understood before it becomes an embedded reality.

2.4 Global leadership

Respondents believed that the UK should learn from other models for digital identity around the globe. The UK was seen as well placed to lead the global discussion on digital identity and could develop global best practice. Respondents believed that, once the UK has established a viable model for digital identity implementation across the economy, the UK should encourage other nations to consider following our approach. Domestic interoperability was considered important but some wanted the UK to work with international partners to grow international interoperability of systems as appropriate.

2.5 Right to redress

A civil society organisation advised that general consumers need a single point of contact to assert their rights or make complaints. Respondents felt specific consumer protections or rights might be needed, suggesting individuals should have a right to redress. Other respondents raised the difficulty of repairing a digital identity and that standards must create a process for stopping the fraudulent use of digital identities. Some do not want digital identity to be implemented at scale until there are clear mitigations to cover worst case scenarios, such as dealing with identity fraud. They stated this would help build trust in how the public view the security of digital identity.

3. Analysis of responses received to each section

This section contains a summary of the evidence provided against each part of our Call for Evidence.

3.1 Needs and problems

Respondents were clear that digital identity would bring benefits to organisations and users. Some cautioned that there is not a clear definition of what 'digital identity' means and that a lack of a common language makes it hard to have a meaningful discussion or frame the debate consistently.

3.2 Benefits

Most evidence regarding the benefits of digital identity related to the economic merits. Respondents identified savings in time and resource as significant benefits, if existing identity checking processes could be partly or fully digitised. Existing methods have security vulnerabilities which respondents felt digital identity could address. Respondents felt that existing repetitive identity proving is time consuming and can be distressing when it comes to accessing some services. Respondents identified repetition as likely to discourage some vulnerable users from accessing services digitally. Respondents saw digital identity improving user experience and as an enabler to help individuals access services they are entitled to without repeatedly needing to prove who they are.

Social benefits were identified. Some responses evidenced how digital identity may minimise discrimination by keeping some attributes secret while providing a credential that meets the needs of a specific purpose.

3.3 User needs

Some cautioned that these benefits could become risks if the legal framework around digital identity is not fit for purpose. One respondent cautioned that a poorly implemented solution, which does not consider a range of user needs, may increase exclusion. Civil society respondents warned that if many organisations are involved in delivering a digital identity it will increase the digital support needed for excluded and vulnerable groups. One charity stated a significant amount of its time is dedicated to supporting vulnerable users to navigate government internet platforms to access to services.

3.4 Authoritative government data

Respondents were clear that authoritative government data is essential to digital identity. Responses identified a need for authoritative government data to be made available. Some stated organisations are unable to fully digitise their identity checking services without the ability to query government datasets. Respondents identified passport data and Driving and Vehicle Licensing Agency data as very important authoritative data sets. However, respondents also mentioned local government data and life event data such as birth certificates. We received evidence that citizens can legally authorise third parties to check government data on their behalf, but are unable to do so in a streamlined way. Some respondents would like a mechanism to better enable this process.

3.5 Criteria for trust

Respondents were in agreement that trust was essential to digital identity becoming a viable solution. Several responses identified that the success of digital identity schemes depended on achieving widespread adoption. Respondents felt the government was best placed to establish consistent

standards, develop meaningful accountability and enforce compliance.

User trust was cited as the most important factor in securing a high uptake of use. It was felt that the government has a clear responsibility to set the ‘rules of the road’ and that the government is best placed to build trust. Several respondents felt certification and assurance were the best model for trust building in technical digital identity solutions.

3.6 Standards

Respondents referenced a variety of existing standards but respondents mostly wanted one set of digital identity standards made up from the best parts of these standards.[4] Some organisations believe a digital identity system based on access to authoritative government data will require bespoke standards. Respondents felt the government must aim for consistent levels of assurance. Some respondents wanted the government to create alignment between existing standards and regulations to enable interoperability and reuse of digital identities across sectors. Others felt further work would be required to make standards robust enough for the demands of making digital identity fully interoperable.

3.7 Accountability

Respondents drew parallels to data protection legislation. Some advocated for a similar body to the Information Commissioner’s Office to build public confidence by being an independent organisation protecting consumer and citizen rights. Respondents linked this idea to accountability, and how users may hold organisations accountable in complex delivery chains. Some felt this would help develop the government and private sector adoption of digital identity and drive acceptance of digital identity by the public.

Some respondents saw transparency as important in building trust, stating that where there are multiple parties involved in a transaction the user should be fully informed and an equal partner in the process. Responses pointed out a need for users to have a choice to build a digital identity in a way that suits their circumstances so that users without a particular attribute, such as a passport, are not disadvantaged. It was suggested the government would be well placed to increase public understanding of how to apply for and use digital identity through an awareness campaign.

3.8 User rights

Some respondents saw meaningful user control of how their data is shared as one way to protect citizen rights. Some stated that services should not be contingent on a digital identity check and there should be an alternative mechanism for those who did not want to share their information digitally.

3.9 New technology

Several technology options including distributive ledgers, biometrics and digital identity wallets were suggested as ways to aid inclusion or safeguard rights. There was not consensus amongst respondents on these technologies, which tended to polarise opinion as advocates and critics provided credible evidence for their particular point of view.

3.10 Role of the government

Most respondents felt the government is better placed than industry to build consensus around a vision for digital identity. Respondents felt strongly that the government should unlock additional data sets. Government data was seen as essential for meeting digital identity needs and could be woven with other data sets if the individual chose. Some requested the government consider the merit and viability of providing a digital token or passport upon request to citizens, suggesting a digital passport could be obtained at the same time as a paper passport. Respondents felt this approach would reduce online fraud and streamline access to government services. Detailed feedback was not received on how digital identity could support the provision of local government services.

3.11 Establishing rules

The majority of respondents want the government to take a lead in setting the rules for digital identity. Consensus on establishing regulation did not carry through to what level of regulation there should be. Opinion was split on if there should be strong regulation or light touch requirements on organisations. Where respondents thought regulation was needed, they stated the government is best placed to develop it. However, a few respondents cautioned against introducing new legal provisions before mapping existing regulation and testing if data protection law was sufficient to cover this area.

3.12 Building public trust

Some respondents, especially those from larger organisations, wanted the government to keep a strict control on who is allowed to undertake checks. Some organisations linked the idea of a closed marketplace to issues of public trust. They argued that only vetted, responsible organisations should be allowed to access government data because the public would lose confidence if it was perceived that irresponsible organisations were making checks against it. Respondents made the case that the government needed to select a delivery model for digital identity and adopt clear policy. These responses argued that a single digital identity format would encourage uptake and reduce costs by establishing a single platform.

3.13 Non-digital identity checking

A small number of individual respondents felt strongly that the government should not promote digital identity and should move away from the digital processing of personal data. These respondents stressed the importance of privacy and that individuals should be able to select identity verification processes that aligned to their needs.

3.14 Role of private sector

In general, responses from the private sector welcomed and encouraged the ambitions stated in the Call for Evidence. When discussing their role, the majority of respondents from the private sector want to work with the government from the outset. Private sector organisations identified that they had a key role in being able to promote uptake within their industries and innovate solutions. Some respondents wanted an open marketplace and felt that the private sector would build digital identity by innovation.

3.15 Liability

Respondents from regulated industries raised the issue of establishing liability if a fraudulent digital identity is used. Some organisations felt that their need to meet the requirements of their regulator and

prove regulatory compliance made the adoption of digital identity tools challenging.

3.16 Cost

Little evidence was provided in relation to cost models. Some stated that costs could focus around the provision of attribute checking and others cautioned against any model where user data was commercialised for any sort of profiling, algorithm training or marketing. A small number of submissions indicated the potential for user data to be commercialised if consent is provided.

4. Next steps

Digital identity is key to enabling individuals to prove who they are securely, online and in-person.

It plays an important role in preventing identity-enabled fraud. In 2018, identity fraud increased by 8% and accounted for 58% of the fraud reported during the same year.[5] Poor identity practice by organisations can be exploited by criminals to commit identity fraud and wider criminal activity, such as money laundering, terrorism and people trafficking.

Stolen documents are an enabler of organised crime, but physical identification is often carried around by people so they can access services. The wide scale adoption of secure digital identity solutions has the potential to reduce this opportunity to steal and use stolen documents.

This government is committed to increasing online security, increasing productivity and boosting the economy. The responses to the Call for Evidence confirm that digital identity is key to delivering these goals. The need for secure, trusted online solutions has only been heightened by the recent Covid-19 pandemic.

Many parts of government have a role to play in digital identity, and have been brought together in a cross-government Strategy Board. This Board guides the work of the Digital Identity teams in the Government Digital Service, focused on the use of digital identity within government, and DCMS, focused on enabling the use of digital identity in the private sector.

4.1 Digital Identity in response to COVID-19

COVID-19 has accelerated changing lifestyles and working habits in the UK. Organisations and individuals had to find a safe digital way to do what they would normally do in person. Ordinary activities like banking, purchasing goods, accessing work computers, getting a prescription sent directly to the pharmacy and taking classes became fully digital activities, done at distance and not face to face. This has accelerated existing trends towards providing physical and digital service channels. Organisations need secure digital identity proofing methods to reduce the repetitive and time consuming need to re-enter information proving an individual’s identity or entitlement to a service.

More agile and resilient public services: Digital identity and the Self-Employment Income Support Scheme (SEISS)

Open to more than 3.4 million self-employed individuals, this scheme was one of a number of initiatives the Chancellor asked HMRC to deliver to support businesses and individuals during the Covid 19 pandemic. HMRC needed most claims to be made online, making digital identity critical

to this service. The department designed it so eligibility of claimants could be confirmed in real time, improving their experience and providing a key mitigation against fraud. Since its launch on 13 May 2020 more than 2.6 million people have made a claim, with 1.4 million having no prior digital identity credential and needing to pass through HMRC's identity verification service. Without an effective digital identity service HMRC would have needed to support claimants through a more manual intervention. This would have made it significantly more complex and expensive to deliver the scheme, and extended the time taken to provide critical financial support.

4.2 A Principles-based approach

Drawing on the call for evidence responses, the Digital Identity Strategy Board has developed principles to frame digital identity delivery and policy in the UK. These principles will be reviewed on an annual basis.

1. **Privacy** – When personal data is accessed citizens will have confidence that there are measures in place to ensure their confidentiality and privacy. Where possible, citizens select what personal data is shared. Organisations will have privacy standards to uphold and will need to prove their ongoing compliance.
2. **Transparency** – Citizens must be able to understand by who, why and when their identity data is used [when using digital identity products].
3. **Inclusivity** – This means those who want or need a digital identity should be able to obtain one. We will look at how citizens could use different attributes (e.g. name, date of birth etc.) held across government and by other parties to support identity proofing.
4. **Interoperability** – Setting technical and operating standards for use across the UK's economy to enable international and domestic interoperability.
5. **Proportionality** – User needs and other considerations such as privacy and security will be balanced so digital identity can be used with confidence across the economy.
6. **Good governance** – Digital identity standards will be linked to government policy and law. Any future regulation will be clear, coherent and align with the government's wider strategic approach to digital regulation.

The principles will inform how the government:

- develops a legal framework to remove regulatory barriers preventing the use of secure digital identities and establish safeguards for citizens
- develops the next generation of digital identity use in government
- explores with citizens how they want to use their government-held identity attributes and how government-held identity attributes can reduce digital exclusion
- promotes a pragmatic approach to international digital identity standards and share best practice to ensure global approach to digital identity aligns with UK digital identity principles
- further enables the secure use of digital identity without the need for ID cards

4.3 Driving forward legislation

Respondents to the Call for Evidence wanted legal certainty on how to use digital identity, and legal gateways to check identity attributes against government data. The government plans to update existing laws on identity checking to enable digital identity to be used in the greatest number of circumstances. The government will consult on developing legislation to set provision for consumer protections relating to digital identity, specific rights for individuals, an ability to seek redress if something goes wrong, and where the responsibility for oversight should lie. The government will also consult on the appropriate privacy and technical standards for secure digital identities. We will look at how to establish sufficient oversight of these standards to build trust and facilitate innovation - providing organisations with a handrail to develop new future facing products.

There is global momentum behind the use of digital identity as a tool to combat harmful practices such as money laundering and terrorist financing. The UK's transposition of the Fifth Anti Money Laundering Directive highlights how digital identities can reduce risks in non face-to-face financial transactions. Future legislation will bring further potential for regulators to authorise the use of digital identity in their context. The government is also considering options to ensure citizen online accounts and data are adequately safeguarded, reducing opportunities for cyber crime and offences that stem from cyber crime.

4.4 Digital identity in government

In the light of the COVID-19 pandemic, which has led to unprecedented demand for key online services using digital identity, the government announced[6] in April that the Cabinet Office could continue GOV.UK Verify operations for up to a further 18 months. Looking beyond GOV.UK Verify, departments have committed to using standards-based digital identity; this will remain critical to the delivery of effective government services online. The government has worked closely with its partners in the public and private sectors to update and publish in 2020 two notable documents: **Good Practice Guide 44** (using authenticators to protect an online service (https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services)) and **Good Practice Guide 45** (how to prove someone's identity (https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual)). These have been welcomed by the digital identity community, and are a key element of establishing a set of standards and rules that would support interoperability across the UK in a secure and consistent way.

4.5 Unlocking government identity attributes

The Call for Evidence highlighted that it would be beneficial to individuals and organisations if existing government-held personal attributes, such as birth certificate or passport data, could be used more readily as part of the digital identity verification process. A Document Checking Service pilot is underway to test the commercial and technical feasibility of responsibly opening up part of the government's authoritative identity data. Throughout the development and selection process for the pilot, there was a high level of industry interest from a broad range of sectors and use cases for the checks. Under the pilot up to eleven private sector organisations are undertaking checks against passport data with the user's permission. Selected organisations are completing the checks as part of services relating to the house buying process, recruitment and financial services, amongst other uses. These results will inform how we expand the ability for individual attribute checking of government data, where associated infrastructure is available, and legally unlock more datasets.

The government is the responsible controller of important authoritative identity datasets and will

continue to ensure data protection standards are met. As more government data is unlocked for use in digital identity, citizens will be able to assert control over how they can prove important facts via attribute checking. User research will be undertaken to understand citizen perception of digital data checking for identity proofing purposes.

4.6 Achieving international interoperability

The Call for Evidence restated the importance of the UK taking an international approach to digital identity. Respondents see the UK as having the experience to lead the development of international best practice. The UK will continue to work with international partners and organisations seeking to enact pragmatic, global standards on digital identity, which prevent digital exclusion and discrimination. The government will support approaches that are technology neutral and protect users.

The government is providing support to countries moving to implement or enhance identification systems through £15 million investment in the World Bank's 'Identification for Development (ID4D)' initiative 2019-2024. Many of the supported countries are low-income and fragile states, in need of more detailed guidance, in-depth and longer-term technical assistance to ensure that their digital identification systems are designed and implemented in a way that fully harnesses their benefits for development while also adequately mitigating the risks.

As part of the Digital Nations Digital Identity Working Group the government is exploring how to make strong e-authentication a global possibility and sharing best practice with member countries.

The government will continue to prevent barriers for UK citizens transacting digitally across borders. The government promotes the following:

- the UK is no longer part of the EU and we exit the transition period, we want UK citizens and businesses to be confident that they can continue to transact digitally across borders. Outputs from e-authentication or e-trust services will continue to have legal effect
- parties to commercial transactions are free to agree appropriate standards for their specific circumstances
- states can introduce performance standards for e-authentication or e-trust services, so long as these standards or regulations are transparent and reasonable
- an independent UK sees benefits in international interoperability and mutual recognition of e-authentication or e-trust services. This will make it easier for UK citizens to safely use digital services, no matter where they are

5. Annex A – Digital Identity: Call for Evidence Questions, July 2019

1. Do you think digital identity checking will be a way to help meet the common needs of individuals and organisations referenced above? What other ideas or options would help?
2. What are the economic or social benefits or costs from developing a digital identity system in the UK which meets these needs? Can you provide examples?
3. What are the costs and burdens of current identity verification processes?
4. How should we ensure inclusion, especially for individuals with thin files?
5. What currently prevents organisations from meeting the needs stated above?

6. Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples?
7. What are the building blocks essential to creating this trust? How should the environment be created to enable this trust – for example, what is the role of open standards (identity, technical, operational, business implementation, design requirements for consumer privacy and protection)?
8. How does assurance and certification help build trust?
9. How do we ensure an approach that protects the privacy of users, and is able to cover a range of technologies and respond appropriately to innovation (such as biometrics)?
10. How do we ensure digital identities comply with the Human Rights Act and ensure people with protected characteristics are able to participate equally?
11. How should the roles, responsibilities and liabilities of players in the digital identity market be governed and framed to enable trust?
12. What's the best model to set the "rules of the road" to ensure creation of this trusted market?
13. Who do you think should be involved in setting these rules?
14. Do you think government should make government documents and/or their associated attributes available in a digital form, which could be used to help assure identity?
15. i) For what purposes should government seek to further open up the validity checking of government-issued documents such as passports? ii) How should this be governed to ensure protection and citizen control of data? iii) What should the cost model be?
16. i) For what purposes should government seek to further open up the attributes (such as age of citizens) that it holds for verification? ii) How should this be governed to ensure protection and citizen control of data? iii) What should the cost model be?
17. What's the role of legislation and statutory regulation to grow and enforce a secure, privacy-centric and trusted digital identity market?
18. What legislation and guidance requires updating to enable greater use of digital identities?
19. What else should government do to enable the wider use of digital identity?
20. How could digital identity support the provision of local government services (including library cards and concessionary travel)?
21. What is the private sector's role in helping to create a trust model (based on the criteria for trust in section 5), and how should they remain involved in its long-term sustainability (for example funding, helping create the rules of the road)?

6. Annex B – List of respondents

Written responses

We received over 100 responses, including from the following organisations. Individual respondents have not been named.

- Accenture

- Association of Document Validation Professionals (ADVP)
- All-Party Parliamentary Group (APPG)
- Amiqus
- Association of British Insurers (ABI)
- Association of Convenience Stores (ACS)
- Atkins
- Aviva
- Avosecure
- Bank of England
- BBFA (British Business Federation Authority)
- Better Identity Coalition
- Billon Group
- Blinking ID
- Broadsail
- BSI Group
- BT Group
- Building Societies Association
- Capgemini
- Caribou Digital
- Confederation of British Industry (CBI)
- CBoxx Ltd
- Cifas
- Citizens Advice
- Citizens Advice Oxford
- CLC (Council for Licensed Conveyancers)
- Cloud Kickers Group
- Consensys
- Consult Hyperion
- Conveyancing Association
- Danube Tech
- Deloitte LLP and Evernym (UK) Ltd
- Digital Identity Net
- Diro Labs Limited (UK)
- Department for Work and Pensions
- Efficient Frontiers International
- Equifax and Digital Identity Net
- Etive Technologies
- Experian
- FIDO Alliance
- Finance & Leasing Associations (FLA)

- Folio Technologies
- GBG
- Goaco
- Global iD
- Global Identity Foundation
- Heathrow Airport
- Helix ID
- HID Global
- Her Majesty’s Passport Office (HMPO)
- HSBC
- Hushmail
- Information Commissioner’s Office (ICO)
- IDEMIA
- IDWorks
- Improvement Service
- Scottish Government
- Singletons Solicitors
- Investment & Life Assurance Group (ILAG)
- iProov
- JISC
- Kantara
- Lead Author British Standard
- LexisNexis Risk Solutions
- Lloyds Banking
- Lockstep Consulting
- Low Carbon Contracts Company (LCCC) and Electricity Settlements Company’s (ESC)
- M&G Prudential
- Mastercard
- Match Group
- medConfidential
- Midas Alliance
- Mydex CIC
- Netis
- Nominet
- Onfido
- Open banking
- Open Identity Exchange (OIX)
- Open Rights Group
- Origo Services Ltd
- Pensions and Lifetime Savings Association (PLSA)

- PIB-d
- Post Office
- Privacy International
- Pyxis Edge
- Reclaim Fund Ltd (RFL)
- Reed Screening
- Refinitiv
- Registers of Scotland (RoS)
- Revolut
- Santander
- SecureKey Technologies
- Self iD
- Signicat
- Sitekit
- Sopra Steria
- Synectics Solutions Ltd
- Target Professional Services Ltd
- techUK
- Telefónica UK Limited
- Thales UK
- The Associated Board of the Royal Schools of Music (ABRSM)
- The Coalition for a Digital Economy (Coadec)
- The Investing and Saving Alliance (TISA)
- The Joint Money Laundering Steering Group (JMLSG)
- The Law Society
- The Money Charity
- The Proof of Age Standards (PASS)
- Thirdfort
- Tony Blair Institute for Global Change
- Transpact
- tScheme
- Ubisecure
- UK Finance
- UK Hospitality
- VChain
- Welsh Government
- Yoti
- YourID

---

1. A full list of questions can be found at Annex A ↩

2. We expect to hold more events in the future and interested parties can register their interest at digital-identity-cfe@dcms.gov.uk ↩
3. In total responses equalled circa 200,000 words ↩
4. Anti-Money Laundering Regulations, Electronic Identity and Trust Services regulation and Good Practice Guide 45 ↩
5. Fraudscape 2019 report, Cifas ↩
6. Written Ministerial Statement, 29 April 2020 (https://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Lords/2020-04-29/HLWS213/) ↩