Department for Digital, Culture, Media & Sport

Cabinet Office

Digital Identity: Call for Evidence

July 2019

1. Digital Identity

Despite all the technological innovation of recent years, proving our identity or something about ourselves often remains difficult, time-consuming and repetitive. When conducting transactions we need to prove our identity to prevent fraud and crime – yet we cannot always be sure the organisation asking for our data is who they claim to be. Equally, they cannot be sure that we are who we say we are, or that the documents we're using to help prove our identity and status are genuine. When seeking access to goods and services, from age-restricted products to state benefits, we need to demonstrate our entitlement. When we disclose our personal data to build trust we also expect to maintain our privacy.

If we could securely and easily prove our identity, or something about ourselves, it would help support innovation, reduce fraud and cost, safeguard our privacy and streamline online services. Whether opening a savings account, buying age-restricted products or paying tax, proving identity should be simple, private and secure.

We are committed to enabling a digital identity system fit for the UK's growing digital economy without the need for identity cards by working in partnership across government, the private and voluntary sectors, academia, and civil society. We see there are significant benefits for citizens and consumers being able to create digital identities under their own control and then to use different verified attributes to access a range of services as and when needed. For instance, I should be able to assert my age to one service, and only my name and address for another service. In this way only information that needs to be shared is exchanged, but the process to ensure this information relates to me and is genuine (identity proofing) only has to happen once.

We want to gather insights and evidence into how government can support improvements in identity verification and support the development and secure use of digital identities and ensure that the potential benefits of this approach are open to all. The evidence we receive will be used to inform policy making and government priorities.

2. Open call for evidence

We welcome written responses to this call for evidence from all interested parties, including citizens and businesses, as well as organisations who anticipate being a consumer or creator of digital identity tools or services, and those focused on protecting civil liberties.

We also encourage responses from individuals or organisations who represent the interests of citizens, vulnerable or otherwise, who are susceptible to being digitally excluded, as well as individuals or organisations who represent citizens with a particular protected characteristic.

In your response, please clarify:

- if you're responding on behalf of an organisation or in a personal capacity
- which questions you're answering, by referring to our numbering system - there's no need to respond to all of the questions if they are not all relevant to you
- whether you're willing to be contacted - if so, please provide contact details

- whether you want your response to remain confidential for commercial or other reasons

If you prefer to engage in person, please tell us. We'll try our best, resources allowing, to find opportunities to do this.

Please provide your response in ODT, DOCX, PDF or similar text format (no more than 2000 words) and send to digital-identity-cfe@culture.gov.uk by 11:59pm BST on Sunday 15th September 2019.

We'll also be holding events with industry and civil society groups during this process to explore the issues in more detail. If you'd like to take part in these, please email your name, organisation and area of interest to digital-identity-cfe@culture.gov.uk by 2 August 2019.

We'll publish a summary of relevant responses later in 2019.

3. Questions

To ensure a structured and comprehensive approach, we've split this document into a series of topics led by brief problem statements or explanatory text and followed with a set of related questions. **We also actively encourage you to include any comments you have on overarching issues such as diversity, digital exclusion, privacy and ethics in the relevant section or woven into your response to a particular section.**

The topics are:

- Needs and problems
- Criteria for trust
- Role of the government
- Role of the private sector

4. Needs and problems

It's often difficult to prove things about ourselves – such as who we are, our nationality, our address or our qualifications. And it's also difficult to prove the person or organisation we're dealing with is who they say they are. If we are a carer, it can be difficult and frustrating to prove that we're acting on behalf of a relative. If we've been a victim of identity theft, it can be time-consuming and distressing to re-establish our identity. Even when we do manage to prove who are we, or something about ourselves, it's often impossible to reuse that proof somewhere else – so we have to do it every time with every person or organisation we deal with.

Some existing laws and regulations stipulate the use of paper documentation and face-to-face meetings, preventing more efficient online processes and the use of digital evidence. Proving identity can be particularly problematic for those without "standard" identity documentation, such as passports, or who have complex lives and personal circumstances.

When we do prove something about ourselves – such as whether we are over 18 or a British citizen – we're often forced to divulge excessive personal information (such as sharing our full date of birth or full passport details). A privacy-centric approach would enable us just to prove a specific fact instead of releasing the underlying data – for example, proving "I'm over 18" instead of providing our full date of birth, or proving "I'm a British citizen" instead of handing over our full passport details. The digital world needs to reflect real-world needs and relationships. There's an opportunity to make things much better and more private and secure than they currently are – but we need to get it right.

While strong identity proofing is essential for some services, for others anonymity and pseudonymity are equally important – when we buy age-restricted products, for example, we do not need to disclose who we are, simply that we're of legal age to do so. The potential benefits of digital identity are not restricted to online transactions – we could prove our age via an app on our smartphones for face-to-face transactions, for example.

Common needs of an individual

I need to prove something about myself (for example I live at a particular address, I'm over 18, I'm legally in the UK, I have a degree or I'm entitled to a benefit) to receive a service, undertake a transaction, take up employment, etc.

I need to act on behalf of someone else (for example via power of attorney or for my employer's business), have someone else act on my behalf (such as an accountant filing my tax return), or have something act on my behalf (for example I want to authorise my wearable health device to update my GP on my blood sugar levels).

I need to know how to do this in a simple way that's convenient for my lifestyle.

I need to know the person or organisation I'm dealing with is who they say they are.

Common needs of an organisation

We need to know something about this individual to deal with them (for example they are over 18, are legally in the UK, have the right to work and are qualified for the job).

We need to know where can we get that knowledge and how can we do it online rather than requiring paper.

We need to know whether it's true (meaning 'What's the level of assurance we have that the information provided is accurate and relates to the individual we're dealing with?') and that it continues to be true in each subsequent transaction.

We need to know how to do this in a data protection compliant and affordable way.

Common blockers include:

- proving identity easily and securely online can be difficult, making it hard to know whether the individual or organisation you're dealing with is who they claim to be
- challenges in proving eligibility to access or receive services securely online
- difficulties in acting on the behalf of another individual or organisation – for example, an elderly relative or a business
- people who do not have many documents that prove their identity (sometimes called "thin file" individuals) struggle to access services
- the fraudulent use of documents commonly used for identification

- organisations storing copies of our personal data, such as passports, increasing the potential for misuse and fraud
- excessive cost to business due to inadequate identification systems and duplicative and time-consuming processes
- complex and distressing experiences when trying to reclaim an identity after being the victim of identity theft

We're keen to gather evidence on how both the private sector and government can support and provide increasingly effective digital identity solutions and have the space and freedom to innovate, while also ensuring that individuals can have trust in the ways that digital identities, and related personal data, are used. In particular we're interested in evidence of the demand for individual-controlled reusable digital identities – trusted identities that can be used in more than one place (contrasting with the current model where a digital identity is only usable with the organisation that provided it).

Questions on needs and problems

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?

5. Criteria for trust

At the heart of a successful approach to digital identity is the need to improve trust between the person or organisation aiming to prove something about themselves, and the person or organisation they're dealing with (the "relying party"). Essential criteria to achieve high levels of trust in digital identity provision include universal coverage (free to the public), standardisation, social inclusion, privacy, data protection, legality, security, proven liability models and consumer protection.

Questions on criteria for trust

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?

6. Role of the government

Government has an essential role to play in enabling secure digital identity solutions for the wider economy. The government and government-appointed regulators already set the rules for identification in many important areas – from passport applications and alcohol licensing to online age verification. The government also provides the primary identity documentation and verification services used as the basis for identity (such as passports), as well as operating identity and authentication services that meet the needs of essential public services such as GOV.UK Verify, HMRC and others (including Government Gateway and NHS Login). Local government also provides many public services that could be improved through digital identity. The public sector is an essential, integral part of any digital identity framework both as a rule-setter and a participant.

The use of public sector held information is critical to the success of digital identity. We anticipate that the use of online services to validate and check government-provided documentation or public sector held data will increase. We are therefore interested in evidence on how best the government should aim to meet demand for access to check the validity of documents or attributes, while ensuring that this is only done with citizens' active consent and control (noting there will be exceptions where required by law). Work on improvements to government infrastructure to enable further validity checking of documents or attributes is subject to feasibility and value for money first being established. This also applies to the creation of digital government documents and their attributes.

Questions on the role of the government

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)?

7. Role of the private sector

The private sector already has a wide range of identity-related services in place. This includes traditional high street banks (and their existing “Know Your Customer” processes), online banking services and new challenger banks, through to companies innovating more generally in the digital identity space. Other initiatives include the Tax Incentivised Savings Association’s work on a digital identity scheme for financial services, the regulatory changes of the Payment Services Directive 2 (PSD2) including Strong Customer Authentication (SCA), and the GOV.UK Verify private sector identity providers. Private sector held data and access to it, for example through the Open Banking initiative, is also used as part of identity assurance (for example data held by banks and credit reference agencies).

Question on the role of the private sector

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)?

8. Further information

Information provided in response to this call for evidence, including personal information, may be published or disclosed in accordance with the access to information regimes. These are primarily the Freedom of Information Act 2000 (FOIA), the Data Protection Act 2018, and the Environmental Information Regulations 2004.

If you want the information you provide to be treated as confidential, please be aware that under the FOIA there’s a statutory Code of Practice with which public authorities must comply and which deals, among other things, with obligations of confidence. In view of this it would be helpful if you could explain to us why you regard the information you have provided as confidential.

If we receive a request for disclosure of the information we will take full account of your explanation, but we cannot give an assurance that confidentiality can be maintained in all circumstances. An automatic confidentiality disclaimer generated by your IT system will not, of itself, be regarded as binding.

We’ll process your personal data in accordance with the Data Protection Act 2018.

Glossary of definitions

Below we aim to provide simplified definitions of the terms as applied in this call for evidence.

Digital identity
A digital identity is information used by computer systems to represent a unique person, organisation, application or device. So for a citizen or consumer, a “digital identity” is a trusted way of proving one or more attributes about themselves online or offline and the linkage of those attributes to that same person as a uniquely identifiable individual.

Attribute
A piece of information about someone. It may be authenticated (such as a marital status that's been confirmed by a trusted source like the General Register Office) or one which may be self-asserted or not independently verified (such as "I wear glasses").

Identity/attribute providers
Attribute providers are the organisations, individuals or other sources who act as the source for information. For example, the Passport Office is the authoritative source for confirming whether a passport and the data on it is valid. A university is the authoritative source for whether someone has the degree they claim. An identity provider (IDP) aims to provide a service where an individual can store and control a collection of attributes about themselves, enabling them to reuse them across more than one relying party.

Relying parties
Relying parties (sometimes known as "service providers") are the individuals or organisations to whom identity or attribute information is being given. For example, an online airline site may ask a citizen for details of a valid passport to be given – they're relying on that information and may want to authenticate the passport data of the traveller.

Privacy notice

The Department for Digital, Culture, Media and Sport (DCMS) is working with the Cabinet Office's Government Digital Service (GDS) on the future of digital identity. Part of this work is a "call for evidence" on what this future should look like.

This privacy notice explains your rights and gives you the information you are entitled to under the Data Protection Act 2018 and the General Data Protection Regulation ("the Data Protection Legislation"). Note that this section only refers to your personal data which we process (such as name, email address and phone number).

Who controls the information you provide?

The call for evidence on digital identity is led by DCMS and GDS. Both organisations jointly control why and how your personal data is processed for the purposes of the call for evidence.

DCMS and GDS have agreed that each of them will take lead responsibility for compliance with data protection laws in respect of the elements of the processing they undertake.

This privacy notice is issued jointly on behalf of DCMS and GDS.

Why are we collecting and processing your personal data?

The personal data we process are the details of individuals who respond to the call for evidence – name, email address and phone number. This is processed by DCMS and GDS for the purposes of the call for evidence, so we can respond to your queries and views. It may also include using your personal data to invite you to events relating to the call for evidence. Finally, there may be a need to follow up in the aftermath of the call for evidence on the same topic or closely related topics.

Our legal basis for processing your personal data

DCMS and GDS are processing your personal data as it is necessary for a task carried out in the public interest.

Who will we share your personal data with?

DCMS and GDS hold the details outlined above on a shared database, and so both are able to access your contact details to enable them to communicate with you regarding the call for evidence. Your personal data will be stored in a secure government IT system.

How long will we keep your personal data?

Your personal data will be retained for one year after the end of the call for evidence period.

Your rights – for example access, rectification, erasure

The data we are collecting is your personal data, and you have the right to:

- see what data we have about you
- ask us to stop using your data but keep it on record
- ask us to stop using and delete your data in certain circumstances
- have all or some of your data corrected
- lodge a complaint with the independent Information Commissioner (ICO) if you think we're not handling your data fairly or in accordance with the law

If you have any of these requests, get in contact with us by emailing digital-identity-cfe@culture.gov.uk.

Questions and complaints

You can contact the ICO through https://ico.org.uk/ or telephone 0303 123 1113.

You can also write to them at:

ICO
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Should you have any concerns or wish to exercise the rights outlined above in respect of the personal data which:

- DCMS is processing, please contact the DCMS Data Protection Officer at dcmsdataprotection@culture.gov.uk
- GDS is processing, please contact the Data Protection Officer at DPO@cabinetoffice.gov.uk

Accuracy

DCMS and GDS take all reasonable steps to keep personal data in its possession or control, which is used on an ongoing basis, accurate, complete, current and relevant, based on the most recent information available to us.

Your personal data will be stored in a secure government IT system.

We rely on you to notify us of any changes to your personal data.

Your personal data will not be sent overseas or used for any automated decision making.

Changes to this notice

We may change this privacy notice. In that case, the “last updated” date at the bottom of this page will change. Any changes to this privacy notice will apply to you and your data as of that date.