BCS, The Chartered Institute for IT's response to DCMS's 'Digital Identity and attributes consultation'

Prepared by Arnoldis Nyamande, Policy Manager, BCS - The Chartered Institute for IT

September 2021

BCS, The Chartered Institute for IT

The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public. We bring together industry, academics, practitioners, and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public. As the professional membership and accreditation body for IT, we serve nearly 60,000 members including practitioners, businesses, academics, and students, in UK and internationally. We accredit the computing degree courses in ninety-eight universities around the UK. As a leading IT qualification body, we offer a range of widely recognised professional and end-user qualifications.

Summary of the BCS position

The digitalisation of ID has merit, with potential to ease bureaucratic processes and enable people living in remote or isolated areas to engage in many critical processes and functions from their homes. However, any move towards a 'digital ID by default' position by UK and devolved governments presents certain risks. Movements towards this position must be developed in consultation with communities and with clear and public equality and accessibility impact assessments across all parts of the proposed framework. Without such safeguards, digital ID has the potential to significantly disenfranchise and compromise the life chances of marginalised communities.

A 2021 Cabinet Office report found that more than 9% of UK adults don't have a valid photo ID, and 2% don't have any form of ID at all[1]. This disproportionately affects older populations, who are less likely than other age groups to hold such ID. In addition, the digital divide means some people may not have the network connection, equipment or skills to take full advantage of digital ID. Closing the digital divide is identified as one of our four key priorities for 2021 – 2025[2]. Contingencies will need to be made to ensure that the digital ID scheme does not further disenfranchise marginalised groups.

While we support the principle of digital ID, its design, development and implementation must happen in partnership with communities and should not replace physical ID at this point. We do not believe there is need for, or sufficient infrastructure to support, removing physical ID in favour of digital ID, rather digital ID should become part of a suite of options available to the public and demonstrate its value over time to safeguard against unintended consequences and disenfranchisement of communities.

BCS is keen to be involved throughout the development of the digital ID scheme, offering the expertise of our staff, members and specialist technical communities[3] to help develop digital ID that works for all who use it.

Below we have provided comment on only the questions most relevant to our areas of interest.

---

[1] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/984918/Photographic_ID_research-_headline_findings_report.pdf
[2] https://www.bcs.org/policy-and-influence/bcs-four-themes-and-campaign-goals-2021-2025/
[3] https://www.bcs.org/membership/member-communities/

Creating a digital identity governance framework

The governing body

1. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

We welcome the proposed governance functions especially in terms of maximising cybersecurity and minimising fraud to ensure data is safe and secure. Our priorities in this area are highlighted in our recent report: 'Priorities for the National AI Strategy[4]'. These are positive proposed steps in the continued efforts to secure the central government data base, to minimise the likelihood of mass identity theft and its consequences.

BCS is working with The Royal Statistical Society, The Royal Academy of Engineering and others to develop industry-wide professional standards for data science to ensure an ethical and well-governed approach so the public can have confidence in how their data is being used[5]. An integral part of the governance function will be the technical frameworks to ensure cybersecurity and maximise trust.

BCS is keen to offer its support to Government in the establishment of the regulator: to inform its functions, appropriate supporting technical framework and in establishing the highest professional and ethical standards.

In reference to the function to 'promote and encourage inclusion', the governing body should build additional inclusion considerations into the trust framework and its certification processes. It should also be able to act if it identifies certain groups are excluded from digital activities or services. The issue of accessibility should be included more explicitly to clarify the term 'Inclusion'. This means not only the accessibility (ease of use by the greatest number) of products and tools aimed at end users (the public) but also the accessibility of products and tools used to generate and manage the products and tools aimed at end users (an accessible environment and systems for disabled staff members).

[4] https://www.bcs.org/media/7562/national-ai-strategy.pdf
[5] https://www.bcs.org/more/about-us/press-office/press-releases/professional-standards-to-be-set-for-data-science/

Trust framework, standards and rules management

2. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

BCS supports the governing body owning the trust framework as aligned; allowing for smoother operations and greater safeguards against events like data breaches.

The identity of the governing body matters. To build and retain public trust, it must be independent from Government, assembled transparently and fairly, and possess the skills, knowledge and experience to safely and securely deliver the highest standards of professionalism, ethics and service.

3. Is there any other guidance that you propose could be incorporated into the trust framework?

We have identified four priorities which should underpin technological and digital innovation:

1. Our digital lives should be in the hands of competent, ethical and accountable professionals

This could be incorporated into the trust framework by ensuring the framework itself and the governing body who manage it are supported by staff who understand the value of ethics in digital and data and how to enact this in practice.

The trust framework must incorporate a robust technical trust-security framework. Trust and adoption will not be maximised unless the trust framework is underpinned by or incorporates a robust technical trust-security framework that is different from those used by companies and governments that have had their data hacked. It must also be easily explainable to the public.

2. Greater diversity and inclusion in the IT profession benefits society

Having a diverse range of staff expertise, skill and backgrounds as well as building diversity into the trust framework will be a strong safeguard against bias and enable it to serve all those who use it to the highest possible standard. Establishing diversity at the heart of the new digital ID environment will minimise the probability of things going wrong and ensure the creation and use of digital Identities reflects the diversity of the UK.

BCS has a Digital Accessibility Specialist Group[6] (DASG), which seeks to enhance awareness of digital accessibility issues. DSAG has worked with the Cabinet Office Advisory Group in the past to develop, promote and co-author initiatives that ensure inclusivity within the digital world; they're a specialist resource available to help further inform the development of this service

3. The Digital Divide is a modern measure of inequality; it can be closed by access to skills as well as technology

The creation and use of digital ID will affect those from marginalised communities who are less likely to have any form of ID. Limiting barriers to access – like cost – and ensuring the trust framework is inclusive and accessible will help deliver this. There should be measures put in place so those without access to technology in their homes or with limited skills can still benefit from digital ID through use of low cost or free options and through making the registration process as inclusive as possible. There would need to be measures in place that would prevent the criminal use of people's IDs without their consent, for example forcing someone to authorise with their fingerprint or autosaved passwords.

Those genuinely encouraging an Inclusive workforce should be aware of the good example from the General Medical Council's, 'Welcomed and Valued'[7] initiative.

---

6 https://www.bcs.org/category/18035

7

4. The world will achieve Net Zero more rapidly with support of digital and data technologies

Digital ID holds potential to revolutionise individuals' access to digital technology, something BCS champions. However, this mustn't come at the cost of the environment; it is paramount that the software and coding used to create and maintain the Digital ID platform is energy efficient. We must also ensure there is in place a strictly enforced Code of Practice, one that pre-empts loop holes people can use to circumvent the law and abuse public trust.

4. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

Establishing a diverse governing body that is representative and reflective of UK society. Widening participation within the governing body and all levels of the organisation will help deliver fairer representation of the interests of civil society, the private and public sectors. Establishing an independent mediator to arbitrate in the event of perceived abuse or conflict may be something the Government would like to consider.

5. Are there any other advisory groups that should be set up in addition to those suggested?

BCS convenes a number of relevant special interest groups able and prepared to support this work including ethics, law and diversity in IT, security, Information risk management and audit, strategy and architecture.

Accreditation and certification

6. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

---

https://www.gmc-uk.org/education/standards-guidance-and-curricula/guidance/welcomed-and-valued

Any organisation bestowed the responsibility of accrediting and certifying ID must, at a minimum, be able to demonstrate the highest standards of professional and ethical conduct as well as meeting comprehensive equality and accessibility standards. Fees and cost must not be a barrier to participation by individuals; innovative approaches to fee structures need to be included so the cost is spread across all those parties that benefit.

Complaints, redress and enforcement

7. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?
8. Do you think there needs to be additional redress routes for consumers using products under the trust framework? (Yes/No)
9. Do you see any challenges to this approach of signposting to existing redress pathways?
10. How should we enhance the 'right to rectification' for trust framework products and services?

11. Should the governing body be granted any of the following additional enforcement powers where the is non-compliance to trust framework requirements?
    a. Monetary fines
    b. Enforced compensation payments to affected customers
    c. Restricting processing and/or provision of digital Identity services
    d. Issue reprimand notices for minor offence with persistent reprimands requiring further investigation
    e. Any further comment _____
12. Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?

Security and Fraud

13. What framework-level fraud and security management initiatives should be put in place?

Inclusion

14. How else can we encourage more inclusive digital Identities?

Removing barriers to access and engagement and building a diverse staff and governance function will foster inclusivity in digital Identities. We believe the greatest achievement for inclusive digital Identities will come through fostering public trust and part of that is when the public can see themselves represented and where decisions are clearly made in collaboration with communities. Similarly, demonstrating that professionals, identifiable through visible standards and accreditation, will be processing their personal data in an ethical manner will encourage trust in digital Identities from all demographics. Giving users the ability to create and control their own digital identities (e.g. through self-sovereign identity) is an approach which may increase trust and, consequently, acceptance and uptake. In addition, contingencies must be made for those who cannot access certain technologies. For example, some people don't receive mobile phone signal from their homes, meaning they can't receive text messages; the system would need to provide an ID across multiple mechanisms.

Trust must be gained by making sure the technology used follows robust security and encryption processes and offers clear, simple and secure approaches to authentication. The trust framework must incorporate a robust technical trust-security framework. Trust and adoption will not be maximised unless the trust framework is underpinned by or incorporates a robust technical trust-security framework that is different from those used by companies and governments that have had their data hacked. It must also be easily explainable to the public.

15. What are the advantages and disadvantages with this exclusion report approach?

It's advantageous in that it shows the progress made by those in the relevant companies and organisations, and allows for the setting of deliverable targets for the future. This encourages accountability and healthy competition.

On the other hand, this may have an adverse impact on organisations with limited resources with which to deliver change.

16. What would you expect the exclusion report to include?

- Confirmation or otherwise that there exists an iterative organisation level process to deliver change
- What iterative measures an organisation has made to improve upon their position annually
- Challenges they've faced since the last report and how they overcame [or plan to] it

Protecting privacy and individuals

17. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

Yes, to ensure minimum standards are met by all accessing the service.

Enabling a legal gateway between public and private sector organisations for data checking
How data could be checked

18. Should disclosure be restricted to a "yes/no'' answer or should we allow more detailed responses if appropriate?

A more detailed response will sometimes be needed; a yes/no approach risks being so binary that it excludes people, acting as the barrier we seek to eradicate.

19. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

Yes, establishing minimum standards against which organisations are measured is fundamental for the maintenance of ethical and professional systems. However, these standards shouldn't be so stringent that they risk excluding those that – for whatever reason – aren't able to meet the standard. Accommodations should be made for those with extenuating circumstances and this should be an iterative process with capacity for review and appeal inbuilt.

20. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

Establishing the validity of digital Identities and attributes

21. Would it be helpful to affirm in legislation that digital Identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

Yes. Parity of esteem for digital forms of ID is important. However for accessibility and inclusion, it is important that physical forms of ID continue to be valid. Legislation must also consider the specificities of how digital ID can be used. For example, will it suffice in place of a signature, or is it just enough to access a digital system? There must also be consideration of what data can be stored in the system and what can be viewed without the owner's consent.