Next steps to DCMS Digital Identity policy development

Thank you for agreeing to participate in one of our listening sessions on digital identity for the UK economy. In advance of your session, we'd be grateful if you would complete the following questionnaire to help ensure your valuable contribution and expertise is fed into the development of the appropriate session, and that where possible, you are allocated the session that is of interest to you.

The questionnaire is broken down into six sections, covering the development of a digital identity Trust Framework, legislation, governance and oversight, attribute checking of government data, international interoperability, and inclusion and privacy. Please don't feel obliged to complete the entire questionnaire if you feel particular sections are not relevant to your interest or specialism. We'd be grateful if you could complete the questionnaire by Monday 12th October.

*Required

1. What is your name? *

Nicole Sandler

2. What organisation do you work for? *

Barclays

3. What is your email address? *

Nicole.sandler@barclays.com

Trust Framework development

In response to the Call for Evidence, the general consensus was that government should take the lead in setting the rules and building public trust. Other countries and markets have developed a trust framework to address these challenges.

A trust framework is a set of rules and standards governing the use of digital identity. All organisations that are part of the trust framework will create products and services, check identities and share attributes in a consistent way, enabling interoperability and increasing public confidence.

4. What thematic areas should be considered in the development of a trust framework and why?

Barclays believes that the following thematic areas should be considered:

1. The person-centricity in the approach (control, privacy)
2. Creating a market-based mechanism for addressing Liability, Legal Frames of Reference, etc.
3. Interoperability (with other initiatives such as self-sovereignty and across geographies)
4. The role of governments / public sector
5. Requirements for use of services (transparency and trust)
6. Reliance / Liability - contractual terms and conditions with customers; restrictions on sale versus use of data

Further, as explained below, Barclays believes that a Self-Sovereign model should be adopted. As part of this Barclays believes Government should develop a framework that enables existing citizens to establish a digital identity using private sector certified providers. Barclays also believes that Government should play a key role in establishing the open standards to be used by these providers to verify a citizen's seed identity, to ensure a consistent high standard of assurance across different providers. This would reassure consumers and firms checking an attribute of identity that the identity has been created to a certain standard and they can therefore trust its provenance.

The process of authenticating a citizen's identity should also be based on open standards that are developed, standardised and commonly used across the economy. Ideally these standards would form part of a global framework to facilitate cross border authentication. These standards would constitute the central foundations of a Self-Sovereign model and should be developed by a wide group of stakeholders across the private sector.

To further instil trust, a clear liability framework should be created to ensure citizens are comfortable that if somethings goes wrong, they have clear recourse.

Finally, trust in a digital identity framework will only truly exist if citizen's have a high level of awareness, and understanding of how the system works, the protections that exist, and the benefits they can receive from using the framework. Ultimately, this understanding will only be achieved through education of the public.

5. Which existing standards or guidance do you think should be referenced?

Please see response to questions 11 and 12.

In addition, it may be worth looking at the technical protocols being looked at by the industry: this is led by the OpenID Foundation, an open, cross sector, non-profit, technology-agnostic, global standards development organisation with liaison agreements in place with ISO, W3C, the US Financial Data Exchange, ITU-T, and others.

---

6. Thinking about UK legislation, international legislation and/or technological developments, what dependencies do you think should be considered in the development of the trust framework?

We do not believe that the trust framework should depend on any specific hardware technology or software platform.

Legislation

Legislation for digital identity is needed to provide a basis of national and international confidence in digital identities. This legislation will be the subject of a formal public consultation, as mentioned in the Call for Evidence response published

on 1 September. Detailed proposals are being developed and may cover the rules and standards that will be part of the Trust Framework, an oversight function for this enabling framework, and the removal of legal barriers to the use of digital identity.

7. What legislative changes and data do you need to enable the use of digital identity tools within your business?

There are a certain pieces of legislation that directly influence digital identities, for example money laundering legislation (e.g. AML Directive), and data protection law (e.g. GDPR). However, government and regulators should review legislation and regulation across the board to see where there may be requirements for physical identity documentation that could be amended to permit acceptance of digital identity as an alternative. In addition, if government looks to base its digital identity framework on a decentralised model using e.g. DLT, it will need to ensure that the legislative framework works with these technological use cases.

Furthermore, legislation should define remediation, transparency and controls, and should ensure that customers have a mechanism to access and review who has had access to what data.

It is important that government looks to learn from countries that have adopted Digital IDs successfully. Models that encompass trust and transparency (e.g. Estonia), and that have been successful commercial partnerships (e.g. amongst banks and TelCos).

Further, beyond legislating to establish a digital identity, there are number of actions that government can take to encourage the use of digital identity. Firstly, education; citizens need to be aware that this digital identity framework exists, understand how it works and why it is safe, and how they can benefit from using it. Government should undertake a major public education campaign to boost awareness across the country and encourage adoption when the framework is established.

8. Where should we prioritise our efforts, and what benefits can we expect to see for people and the economy?

With respects to the private sector, if an effective digital identity framework were to be comprehensively introduced, the potential benefits are vast. From a consumer experience perspective, the ability to prove who they are to a firm quickly, easily, and securely using a digital identity, can save significant time and effort compared to current manual processes that prevail. Similarly, from a business perspective, more and more activity that requires identity verification is being conducted online. A digital identity framework enabling firms to efficiently and securely prove a consumer's identity online, without the need for physical documents, would likely provide a significant boost for innovation across the economy, while simultaneously reducing the fraud levels and costs that industry currently incurs to manually prove consumers' identities.

Barclays believes that digital identity has the potential to provide significant value for consumers, businesses and for the economy as a whole. Further, it is crucial to the embedding of the system as a whole, that citizens' digital identities be available for use, and re-use, across the private sector. Barclays strongly believes that the private sector market should drive where a digital identity could be introduced and be beneficial, rather than being limited or restricted by Government, however the public sector is a good candidate for the initial scale and adoption of such a solution. This will enable a truly 'create-once, re-use many times' approach.

Further, identity should no longer be treated as a function-based requirement and instead should be viewed as a commercial opportunity to not only improve core efficiencies but also to deliver consumer value.

Specifically, Barclays believes that government should prioritise efforts on a 'Self-Sovereign' model of digital identity as this would provide significant benefits including: (i) citizen's would control their own digital identity, and can determine what data or attributes they choose to share, boosting privacy; (ii) efficiency of identity verification is increased, for both consumers and organisations; (ii) innovative new services would emerge; and (iv) costs of existing identity verification processes would be removed.

Lastly, we believe that the digital economy is fundamentally a platform economy. That is to say, digital identity enables not just banks to secure the end points of financial transactions, but for all companies to appropriately and responsibly use attributes from identities, secure in the knowledge that they are rooted in trust. Such a platform model will create business opportunities and provide for new services. Part of the rationale for a Self-Sovereign model is that creating a centralised or federated model will not only have scale challenges but also be a valuable attack target. We

understand others *may* have differing views, so we believe that government should encourage multiple models to participate – or at least not preclude options.

Governance oversight

A governance and oversight function will be helpful to enable the safe creation and use of digital identities across the economy, and provide guidance if something goes wrong.

9. What should be the tools available to an oversight body to ensure adherence to the Trust Framework?

Please see our response to question 10.

---

10. What should be the consequences for infringements of the agreed Trust Framework?

Whilst fines may be one potential consequence for infringement, Barclays believes that fines may not always be sufficient. One potential consequence, if a breach is severe, is to be unable to participate in the Trust Framework. Further consideration may be required relating to user consent to data retention/access. This could include for instance, implementing proper controls for revocation and lineage management (in the case of data compromise) and the need for clear management of end of life access (managing access in case of data revocation).

How should redress be handled for organisations that consume digital identity, and for people if something goes wrong?

Organisations often seek to strike a balance between ensuring a good customer sign up journey (to encourage adoption / reduce dropouts), with a robust identity verification process to reduce fraud / abuse.

Organisations often choose to not verify the identity of individuals, which can ultimately have far-reaching knock-on effects. For example, social media organisations do not currently verify the identity of their users, presumably because this would add complexity and friction to the sign up journey, which they want to avoid. However, this is leading to abuse of these services, as outlined in the Government's Online Harms white paper. If there were a simple and quick way for an individual to prove their identity online, these social media organisations could be required to perform Know Your Customer checks, to ensure that they are aware of the identity that sits behind a profile (even if that individual chooses not to share that information publicly). This could allow recourse for online abuse, and other criminal activity such as scams and fraud, that are currently rife across these platforms.

11. What existing bodies or groups may be well placed to provide oversight?

Barclays would recommend mirroring the consultative governance structure that has helped to shape the delivery of Open Banking. Established institutions, Third Party Providers (TPPs), and consumer and SME representatives have worked with technology experts and a central organising entity established to develop the standards, guidance and frameworks that have facilitated the implementation of the initiative. Working Groups were established with specific focus areas, such as technical standards development, legal, data security and fraud, to bring together experts in these fields to rapidly problem-solve as new challenges were identified. Customer research has been undertaken at key stages, to ensure that priorities such as consent, transparency and control have been delivered to customers' expectations. This approach has encouraged all players within the ecosystem, both current and new, to be involved in the development and delivery of the standards and best practices, which in turn has led to better customer outcomes. By focusing on the needs of all sections of the market, a realistic, balanced and customer-outcome driven approach has been made possible. When considering establishing an approach for digital identity, Government should consider which key areas of expertise would be required; in addition to those above, we would expect this to include e.g. cyber security and cryptography. As noted above we also recommend learning from other jurisdictions such as Estonia.

12. It is envisaged that an advisory group will be created to provide viewpoints from industry and privacy groups - how could this be best enabled?

Barclays believes that an Advisory Group would be beneficial. Thematic working groups should be established comprising of relevant experts from across society and the economy to tackle particular challenges. It is important that the initiative has full buy in and all relevant stakeholders are involved to help shape and develop it from the outset.

One suggestion would be to form something akin to the European Commission's Regulatory Obstacles to Financial Innovation Expert Group (ROFIEG) or the US Fed's FinTech Advisory Board. The Group (consisting of private sector entities and public sector participants and/or observers) would meet e.g. monthly / every 6-8 weeks and provide recommendations on key thematic areas.

Attribute checking of data

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. government

13. What attribute datasets would be useful for your organisation (beyond passports and driving licences)?

Barclays believe in a self-sovereign, platform based approach. In this model, the customer would self-select verifiable attributes that are interesting to companies that they want to work with. The identity platform would verify that they are who they say they are, and that the attribute is valid, but have no strong perspective beyond that. We think this will enable a vibrant economy of companies using identity. For example:

- A tenant can populate their identity with verification from their current landlord on the timeliness of payments. Such a record can be used by future landlords.
- A prospective employee can populate their identity with their qualifications and verified employment at prior employers. This can then be used by future employers.
- A specialist can access health records as well as personal health data generated by wearables.

---

14. How likely is it that your organisation will invest to enable checks against government identity data when it is available?

---

15. What is the commercially viable price point for your organisation to make a single check against an attribute dataset?

The self-sovereign model decentralises the cost, which is appropriate since the value of the ‘check’ is variable, as is the risk. For instance, an employment check, or a check for a car loan in a dealership, carriers higher risk (and presumably higher cost) than checking if you are over 18 in a supermarket when buying alcohol.

---

16. Which type of digital identity checks would be most useful to your service model? E.g. are 'yes/no' validity checks relating to data inputted by your customer sufficient? Are photo or fuzzy matching essential components?

A self-sovereign model is extensible to allow for many different kinds of data types and matching models.

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.

17. How important to you is international interoperability?

Mark only one oval.

	1	2	3	4	5	
Not important	○	○	○	○	●	Very important

18. With which markets is it particularly important for the UK to achieve interoperability?

The aim should be all markets but as a starting point, we believe key markets would include: US, EU, APAC (i.e. Japan, Singapore, India and Australia)

Privacy and inclusion

Respondents have highlighted privacy, inclusivity, and proportionality as three of the key principles underpinning the development of digital identity for the economy.

19. What are your concerns about consumer protection and privacy in developing a new digital identity trust framework?

There is a tension that exists between innovation and data protection. Barclays believes that a self-sovereign model would protect the privacy of citizens by nature of its design. By having, a competitive market place for identity verification and ongoing authentication there will be a stimulus for those market players to continue to innovate the methods that they use, within the established guidelines. As well as the commercial and consumer drivers for privacy, the overarching governance body could be responsible for monitoring and enforcing the privacy principles. To add further colour, the citizen would be in control of their digital identity, and would insource additional identity attributes from different sources to develop their identity. Under a self-sovereign model, entities looking to determine a citizen's identity or an attribute of their identity do not need to establish and hold data themselves – they hold the minimum data necessary. Instead they would make an inquiry of the identity controlled by the citizen, which then confirms using data from multiple sources that they are who they claim to be. A citizen never shares more data than is required. Currently, a citizen wanting to prove they are over 18 in order to buy alcohol may provide their physical driving licence. While this may confirm the citizen is over 18, it also reveals the customers actual age, as well as much more data that it is unnecessary to reveal. A self-sovereign model would enable a specific inquiry about an identity attribute of a citizen to be met only with a confirmation or rejection, without having to provide extra information provided on a driving licence, for example.

After a citizen's identity has been verified, they can be subsequently authenticated using biometrics on a user's device, or any other range of authentication methods that may develop over time. Further, we expect a market to develop around authentication.

20. Do you already have practices implemented into your service that focus on diversity, inclusion and safeguarding (e.g. in policies or embedded into technology)? If yes, please provide examples. If not, have you encountered any barriers in trying to do so?

21. What could government do to help ensure digital identity is as inclusive as possible?

Barclays recognises that citizens with 'thin files' may currently face difficulties in verifying their identity. Barclays believes the creation of a self-sovereign model of digital identity would provide a solution to this problem. For instance, Government would issue seed identities for all new births, and the private sector would be commissioned to issue identities to existing citizens. Government will need to consider how these initial seed identities can be provided to citizens with 'thin files'. Additionally, this process would only need to be completed once for each citizen, and then once they have their digital identity, this will significantly reduce the challenges that many 'thin-file' individuals face in today's society, as they will be able to use this digital identity to prove who they are in a range of circumstances. The opening-up of Government data to electronic checking will hopefully help to solve the problem for individuals with thin files.

Beyond thin file citizens, there is the issue of inclusion from a digital accessibility perspective. Many citizens do not have access to the internet or a smart phone. When considering authentication methods, it is likely that there will need to be a number of options to suit the needs of all citizens. For example, banks provide their customers with a range of authentication tools, from entering a code or thumbprint on their mobile device, to using a card with a PIN, to using an offline hardware token. Government could therefore work with the private sector to identify ways to enable an individual to authenticate (and therefore reuse) their digital identity. We would also expect a commercial market to develop around authentication, enabling simpler authentication methods to be used in certain scenarios, where a lower level of authentication is suitable.

22. What are your key accessibility concerns in the area of digital identity?

We anticipate that the listening sessions will commence from 21st October. Please indicate below the topics that are of most interest to you. Please tick all that apply.

23. What topics are you most interested in exploring during the listening sessions? *

Tick all that apply.

- [ ] Trust Framework development
- [ ] Legislation
- [ ] Governance and oversight
- [ ] Attribute checking of government data
- [ ] International interoperability
- [ ] Privacy and inclusion