ABI Response to DCMS & Cabinet Office Call for Input Regarding Digital Identity

Introduction

The ABI is the voice of the UK's world leading insurance and long-term savings industry. A productive, inclusive and thriving sector, we are an industry that provides peace of mind to households and businesses across the UK and powers the growth of local and regional economies by enabling trade, risk taking, investment and innovation. The UK insurance industry is the largest in Europe and the fourth largest in the world. It is an essential part of the UK's economic strength, managing investments of over £1.8 trillion and paying nearly £12bn in taxes to the Government. It employs around 300,000 individuals, of which around a third are employed directly by providers with the remainder in auxiliary services such as broking.

Executive Summary

The appropriate provision of Digital Identity has the capacity to transform the way that consumers interact with services across the economy. A number of solutions have grown organically in different sectors, but due to the patchwork of regulations that currently govern digital ID they are for the most part limited to their particular sector of the economy. This need not be the case and this call for input should be the first step in ensuring that the UK develops an economy wide approach to digital ID.

The best way to ensure that the whole of society benefits from the promise of digital ID is by establishing a system of open standards that can provide security, certainty and usability. This may require the creation of a new independent authority with a duty to minimise risk to consumers and ensure that new technology can be incorporated into the ecosystem.

An independent authority with sufficient backing from central government can act as a catalyst and co-ordinator for new projects that require co-operation across government and industry. For example, GDS played an important role in the early pensions dashboards projects. Similarly, there is potential for future technology solutions like pensions dashboards, which would enable citizens to use one party to access data about them held by another party using a common digital identity. The involvement of a credible public authority in these projects is particularly important to demonstrate legitimacy, especially where the data is held by a public body.

A functioning market in digital ID has the capacity to dramatically reduce risk and cost within financial services and the wider economy. By increasing the level of certainty for relying parties and removing physical processes it can change the way in which certain types of risks are managed. This increased market efficiency will benefit everyone, and we look forward to working with government and wider industry to make it a reality.

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?*

A well-defined and operationally strong digital ID market would meet all of the needs mentioned above.

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?*

There are a variety of economic benefits that could come from developing a strong digital ID solution that can be used in a variety of circumstances. If reusable digital ID can replace certain processes, like wet signatures and sending of verified photocopies of physical documents via white mail, this could drive efficiencies in the administration of financial services. It could also help to tackle issues as diverse as prescription and ticket resale fraud.
The processes mentioned above are essentially due diligence processes that are designed to mitigate the risk of fraud or the use of financial products to launder the proceeds of crime. Many of these processes utilise a risk-based approach set out by JMLSG and require businesses to make proportionate decisions. Digital ID can make this system safer and more efficient by removing the costly processes mentioned above and reducing risk. This also has the additional social benefit of making certain types of financial crime harder to perpetrate.
It is likely that the UK economy will increasingly rely on digital transactions so safe and properly authorised data sharing and a clear definition of the benefits will be an important part of economic growth. This does raise a civil rights issue; namely how do we ensure that individuals not only remain in control of their personal data, but are able to use it for their own benefit. The General Data Protection Regulation [GDPR] has provided a framework for protecting the individual, and the proper provision of digital identity could give the individual the ability to easily use their data to their advantage. This is already happening in other areas through projects like Open Banking and pensions dashboards, giving consumers access to their financial data when they want it and in a manner of their choosing.

3. *What are the costs and burdens of current identity verification processes?*

Physical processes are inherently inefficient as previously mentioned and the current regulatory regime does not provide the certainty that some businesses need from digital ID. There is currently a matrix of different requirements between good practice guides 44 and 45, JMLSG guidance and the “Strong Customer Authentication” required by PSD2. This creates a degree of uncertainty which is in itself a burden.
The private sector is making good progress in establishing standards and schemes that help resolve these issues, but there is a role for government to establish an overarching structure.

4. *How should we ensure inclusion, especially for individuals with thin files?*

Whilst the use of digital ID should become the norm, it is important that other methods of establishing identity are retained for those who are either uncomfortable using these services or who lack the data footprint to properly verify themselves in the usual manner. For the latter case, services that allow them to create a digital identity through other means should be developed.

5. *What currently prevents organisations from meeting the needs stated above?*

There are several factors that prevent organisations from meeting the stated needs. The aforementioned lack of coordination between the different regulations regarding digital ID makes it difficult to design products with wider usability. Another potential hindrance is the presence of legislation and regulation that precludes the use of digital ID due to being passed before digital ID was a reality. Outside of the Verify framework, Digital ID providers currently do not have access to certified government databases like DVLA and HMPO, that could provide a much higher degree of clarity than is currently available when verifying official documents.

6. *Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples?*

As well benefits in terms of efficiency and fraud reduction, another way in which reusable digital ID can add value is by providing certainty to service providers that terms and conditions have been agreed to. This can be particularly hard to prove when business is placed through intermediaries like brokers and advisers. A process where customers digitally sign off on the data and terms and conditions would streamline processes and lower risk for providers. Another use we would like to explore is to enable financial services providers to access the Office of the Public Guardian's Powers of Attorney register online with a customer's consent. In turn, it may be possible for the OPG to access providers' data with the customer's consent. This solution could also allow customers to upload Power of Attorney documents to the online register, to streamline the notification process.

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)?*

There are two different types of trust that have to be engendered before the market in digital ID can be considered a success. Consumer trust, and the trust of businesses using or relying upon the products. Consumers use digital identity products for a wide variety of services currently, but they are all relatively low value, or individual transactions such as e-commerce. For digital ID to become more widely accepted for more significant services,

such as transferring assets, a government endorsed framework may be necessary to reassure consumers that their data is being used appropriately.

In order for relying parties to trust a system or scheme a clear framework needs to be established that creates certainty with regard to liability and the legal position more widely. The best way to do this would be through an independent authority managing open standards. The use of open standards has become a central part of the development of the UK economy. Open banking-based applications have demonstrated how a combination of high technical standards combined with strong tests from fitness and propriety can lead to innovation and the creation of value. It is crucial that any future developments in the digital ID market are also based on open standards so that consumers can be served best by a competitive market. We would be glad of the opportunity to contribute further to this work.

8. *How does assurance and certification help build trust?*

Assurance and certification both have a key role to play in building trust. A clearly defined, and recognised certification process will provide businesses with a trusted standard to meet their needs and a system of assurance will ensure that the standards of the certification are maintained. A kitemark as part of the certification process could also be helpful in reassuring consumers that any provider had been assessed by government.

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)?*

An independent authority could be established that with a duty to protect consumers and maintain a modern market that reflects changes in technology. We suggest there would need to be extensive engagement with stakeholders across different industries affected, as well as with privacy groups, consumer groups, and others. If correctly structured this authority could engage extensively across the economy and encourage the growth of technologies that generate real value for consumers and businesses.

10. *How do we ensure digital identities comply with the Human Rights Act and ensure people with protected characteristics are able to participate equally?*

Ensuring that people with protected characteristics are able to engage with the digital economy should be a priority for both business and government. Much like consumers with a “thin file” alternative processes and special considerations should be given to those who would otherwise struggle to access services. We suggest further due diligence be carried out on this issue both before, and throughout the design of this process.

11. *How should the roles, responsibilities and liabilities of players in the digital identity market be governed and framed to enable trust?*

This is a wider and more complex question than can be fully answered in this consultation. It is likely that the best way to resolve these issues would be through the creation of an independent authority that is tasked with managing the roles and responsibilities of the respective parties within the ecosystem. We suggest that if Government designates an independent authority, they consult on this with interested stakeholders.

12. What's the best model to set the "rules of the road" to ensure creation of this trusted market?

The best model to "set the rules of the road" would be the creation of an independent authority. The current patchwork of regulation has not led to the creation of a fully functional market, and a new authority could set the open standards that will bring about the economic benefits that digital ID promises. This authority should consult heavily with all stakeholders to create a system based on consensus.

13. Who do you think should be involved in setting these rules?

As mentioned above, we think that it is necessary to create an independent authority to set the "rules of the road". It is also vitally important that all stakeholders are involved in the creation of these rules, including and not limited to the following;

- Providers of digital ID solutions
- Service providers (both financial and other)
- Consumer groups
- Regulators

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?

There are a number of circumstances where we believe it would be appropriate for government to make documents available for the purposes of identity assurance. There is likely to be a small degree of risk attached to using digital ID, just as there is with any other form of identification. The aim of any new framework that is established should be to ensure that any risk is minimised, costs are proportionate, and user experience is optimal. Allowing well-regulated firms with a high degree of technical acumen to access government documents with the permission of the consumer would allow firms to greatly reduce the risk of fraud. For highly regulated businesses this could mean having to hold less capital to mitigate these risks, which could make products cheaper for the end user.

15. i) For what purposes should government seek to further open up the validity checking of government-issued documents such as passports?

The ability to check the validity of government issued documents should be extended to those who have to rely on them for a variety of reasons including due diligence purposes or justified intention to provide public good. For example, it could be used by those who are under a legal requirement to check residency status and for verifying a customer's identity at a new address to reunite them with their savings.

ii) How should this be governed to ensure protection and citizen control of data?

These kinds of checks should be managed in a similar way to other data rights like those set out in the Data Protection Act 2018. Consent should be the underlying principle with consumers only having their documents checked if they are entering into a transaction which requires it and they give consent to the process. We think this is an issue which an independent authority should consider.

iii) What should the cost model be?

This should be determined by consultation once a framework has been established.

16. i) For what purposes should government seek to further open up the attributes (such as age of citizens) that it holds for verification?

One way in which use of attributes would be of value is in helping to reunite consumers with savings that they are no longer in contact with, an issue which is particularly prevalent when a customer moves and does not inform their provider of their new contact information. Currently a provider has to carry out a range of tracing activity to attempt to reunite a customer with their funds. Providers can trace customers with a high degree of accuracy to a suspected new address though confirming this information is a more challenging, though necessary step in the process. We would like the ability to be able to verify a customers address against Government data in to support reunification efforts. Providers estimate the reconnection rate could increase from around 35% to around 85%. Please see the Annex for the full proposal.

ii) How should this be governed to ensure protection and citizen control of data?

As mentioned in the answer to 15 ii, a similar regime to data protection should be adopted, with a clear legal bases for use. We also believe there is a role for an independent authority in ensuring compliance.

iii) What should the cost model be?

As a rule, the cost of attribute sharing should not fall on the consumer. We think further work would need to be carried out around the distribution of the cost burden.

17. What's the role of legislation and statutory regulation to grow and enforce a secure, privacy-centric and trusted digital identity market?

There is already a great deal of legislation and regulation that affects the market in digital identity. The role of legislation should be to establish a methodology for making this regulation consistent, proportionate, and above all fit for use by consumers and businesses. We urge the Government to consider the regulation already in place to ensure clarity for industry and stakeholders, and to reduce any implementation challenges.

18. What legislation and guidance requires updating to enable greater use of digital identities?

The most obvious candidate for updating would be the guidance issued by JMSLG. Properly setting out expectations around how digital ID can be incorporated into the risk-based approach is essential. It may also be necessary to implement a “catch all clause” to ensure that all legislation that refers to the need to prove identity is suitably updated.

19. What else should government do to enable the wider use of digital identity?

Government should make clear that the expected method of identifying consumers should be digital and that it is unacceptable to refuse to do so. Whether the check is for AML purposes, checking residential status and current address or ensuring that a consumer has a driving licence, the expectation should be that it will be achieved through digital means. This should be qualified by our answers to earlier questions regarding protected characteristics and “thin file” consumers.

20. How could digital identity support the provision of local government services (including library cards and concessionary travel)?

Local government provides vital services to communities in a time of budgetary restraint. They therefore have to ensure that they provide services to those who are entitled to them. A functioning market in digital ID should reduce the cost of verification, the ability of fraudsters to take advantage of customers, and open up new opportunities around access to services. There will still be a need to offer services to those who cannot, or choose not to participate through digital means.

Role of the Private Sector

21. *What is the private sectors role in helping create a trust model (based on criteria for trust in section 5), and how should they remain involved in it’s long term sustainability (for example funding, helping create the rules of the road)?*

The role of the private sector should be to contribute to the creation of the trust model as a valued stakeholder, promote uptake within their respective industries, and then abide by the rules of the road once they are set by an independent authority. It may be worthwhile for government to incentivise the adoption of digital ID in some circumstances. It is likely that the creation of rules regarding digital identity will be iterative, and industry should be involved throughout. Long term sustainability depends on funding and usage which in turn depend on usability and trust. It is a principal in other types of regulation, that regulated parties pay for the cost of their regulation, and we think this could also be the principle here.