DCMS Digital Identity Policy Development – Sage Submission

November 2020

About Sage

Sage is the UK's largest technology company and the global market leader for software that provides small and medium businesses (SMEs) with the visibility, flexibility, and efficiency to manage finances, operations, and people. This technology includes integrated accounting, payroll and HR native cloud systems, as well as on-premise and connected cloud.

We are passionate supporters of the UK's small and medium sized business community. Our 2,500 Sage colleagues in the UK support over 1 million SMEs through our products, partners, and advice.

Introduction

Sage welcomes the important and timely opportunity to provide input into the UK's policy development of a digital identity. Digital adoption is integral to business success and therefore we welcome an approach that could potentially open up new opportunities for SMEs, streamline processes and drive productivity.

Since the beginning of the pandemic, Sage has regularly polled SMEs and learnt of the significant negative impact on sales, productivity and operations as well as the challenges in access to finance and difficult decisions around the future of their workforce.

Coming into the crisis, our research showed that just 20% of SME processes had been fully digitised and just 50% of businesses were investing in technology as a priority. Contrast this with the past 6 months, where 73% of businesses have adopted new technology.

As both government and businesses face continued uncertainty and disruption in the wake of COVID-19, the need for greater digital adoption in the UK has only become more pressing. Businesses and government agencies alike have had to radically change their plans and strategies to adapt to unprecedented ways of working. Yet barriers still exist in remaining compliant and accessing finance, payments and support, which a digital identity could go a long way to address.

Sage supports the development of a digital identity that would enable government and businesses of all sizes to further digitize their processes and increase both efficiencies and productivity across the economy.

Sage believes that a digital identity can be an important vehicle to realizing the objectives set out in the UK National Data and Digital Strategies and the Bank of England's Open Data for SMEs Initiative, while underscoring the need for interoperability.

The key to unlocking value for both individuals and businesses is its applicability across the entire economy. A digital identity that can be used by both groups will be essential, especially as lines are often blurred between our personal and professional lives. Further clarification is needed on what would be the relationship between individual and organisational identities, especially when interacting with institutions and third parties and how that data would be owned and governed.

For the purpose of the DCMS Digital Identity Policy Development, Sage is focusing on the benefits for and applicability of a digital identity for SMEs.

Key considerations

Accessibility to private sector organisations

From the perspective of SMEs and organisations like Sage, who serves them, the most fundamental requirement of a digital identity scheme is that private sector organisations can participate in the scheme as relying parties. The previous GOV.UK Verify scheme limited private sector participation as only identity providers. A more open approach would support many known opportunities for streamlining business operations and increasing reliability and trust. It would also undoubtedly unlock innovative solutions and services that we cannot anticipate.

Relationships between individual identities and organisational identities

Sage calls on Government to prioritize both individual and organisational identities in order to deliver productivity across the economy. The development of an organisational identity as referenced in initiatives such as the Bank of England on Open Data for SME Finance[1], depend on a unique identifier for organisations, often referred to as a Legal Entity Identifier (LEI). However, many activities related to organisations (such as tax reporting) are ultimately initiated by individuals. There is a strong real-world link between the identity of individuals and the identity of organisations they represent, work for or interact with. We believe that this link should be explicitly recognised and addressed from the outset by both the DCMS digital identity scheme and related initiatives such as the Bank of England's Open Data work. While recognising that this may introduce some short-term complexity, we believe that if these initiatives are allowed to develop independently, it will inevitably result in longer-term complexity for SMEs and missed opportunities for streamlining and increased trust.

Clarity on liabilities

If individuals, institutions and organisations are relying on digital identity to make decisions, then it follows that they are exposed to some level of risk should any aspect of the identity be incorrect - either due to human error or malicious actions. In order to manage these risks, further clarity is needed on liabilities. As TechUK observed in it 2019 White Paper, there are different schools of thought on liability models for digital identities. Sage recognises the potential benefits of the Trust Model, where the liability for a multipurpose digital identity is based on a set of minimum operating rules, common global standards, a global and scalable network and an application framework that is open to all providers. However, Sage also reaffirms TechUKs view that further examination on all models is needed.

Agility in standards evolutions

From a technical standpoint, the area of digital identity is evolving very rapidly, with new standards and approaches gaining acceptance and then receding relatively quickly (e.g. the rapid transition from OAuth 1.0 to OAuth 2.0 and the backwards compatibility between the two standards). At the same time, the threat landscape is also quickly evolving as criminals continually look for new opportunities. Overall, the impact of this rapid evolution is positive for trust and security, but it makes it difficult for standards organisations to stay relevant. Any governance or standards framework for a digital identity must take this into account and strike the right balance between maintenance of standards and agility. In particular, any legislation involved should aim to be as light-touch as possible and allow standards to evolve quickly in response to the changing technology and threat landscape.

International vs UK view

In general, the wider the adoption of any framework or standards, the more effective they are. On the other hand, when more parties and perspectives are involved, it becomes more difficult to achieve consensus without watering the standards down by making them less specific.

In the case of a digital identity, there are significant potential benefits for UK SMEs and individuals from a UK only framework, that presumably could be achieved more simply and quickly than a more internationally focused framework. This is reinforced by the inherent uncertainties that result from the rapid evolution in the technical landscape around digital identity – any standard that takes a long time to agree, risks becoming obsolete before it is even adopted. On the other hand, in a UK that aims to be increasingly global in its outlook, we cannot ignore the international picture. This is a difficult balance to achieve, but it is essential for the long-term success of digital identity.

Proportionate cost of access
A successful digital identity platform will be used in a wide variety of ways – ranging from relatively low risk scenarios to much higher risk ones. This diversity of use cases will be a strength of the platform, but it suggests some complexity in the cost of access, especially for relying parties from the private sector.

For high risk, high value scenarios, a relatively high cost of access may be acceptable, but for low risk, low value scenarios, it will not. In fact, in many low value scenarios, any cost at all is likely to impede adoption while social identity remains free to consume. The cost model for the digital identity platform must reflect this.

Thematic principles

Sage supports the Government's initiative to develop a digital identity and believes the 6 principles will be fundamental to its success with a special emphasis on the importance of:

Inclusivity – People and businesses should be empowered to obtain a digital identity. It should be easy to access, set up and use. Consideration must be given to the local, small and micro businesses that still largely rely on manual processes. In a recent Sage report on Digital Adoption during the COVID-19 pandemic, only 57 % of small businesses indicated that they use their highest priority technologies regularly. If the government does not take further steps to incentivize and enable businesses, there is the risk that some businesses will be left behind, and the full potential of this initiative will be unrealized.

Interoperability – Clear standards will enable interoperability in both the public and private sectors. Interoperability and mutual standards will reduce fragmentation and lead to more widespread uptake. The interoperability of the digital identity underpins the success of other government initiatives like Open Banking and the National Data and Digital Strategies. Aligned with these strategies, the creation of standards should be led by a consumer-first mentality.

Privacy – Individual consent must be established for data linked to a digital identity with the option to withdraw consent and potentially remove access to their data. The individual should be aware of who owns the data once it is shared, what it is being used for and how to request their digital identity be removed from the data, rendering it anonymous. A recent Sage survey on SME attitudes towards data revealed that whilst all SMEs see data as vital to the success of their business, 80% of SME's want more control of their data, and that trust in data sharing, data security and data privacy were the biggest barriers to subscribing to a service. We should be mindful of this hesitation and issues of data ownership, privacy and security should be addressed from the outset.

In addition to the 6 principles themes, Sage would like to underscore the importance of:

Authenticity - The digital identity needs to be verified and authenticated with a transparent and auditable degree of assurance. High assurance digital identity must correspond to both the government and private sector institutions' standards for initial registration and for subsequent acceptance for a multitude of civic and economic uses. The data requirements should be tiered in the legislation and its verification should correspond to a level of confidence and authentication. Biometric data could be used as a token.

SME Adoption

The development of a robust and interoperable digital identity framework can provide greater inclusion, formalisation and digitization for SMEs. More specifically, it could enable the following benefits:

- Greater connectivity among businesses, through the streamlining of services from business to consumer (B2C) and business to business (B2B)
- Enhanced productivity and competitiveness
- Enhanced quality and availability to data
- Greater access to finance through e-KYC
- Increased provision of services
- Enhanced trust across organisations and industries
- Less instances of fraud

Examples

Setting up a business
The development of a digital identity could provide for a more seamless registration and authentication process for new businesses. Setting up a business requires that an identity is established through multiple exchanges with banks, accountants, tax authorities and other stakeholders. There is often a need to demonstrate identity during this process, for example to comply with anti-money laundering legislation or create new legal entities. A digital identity that can be shared with different stakeholders would simplify the process, make it less error prone, and provide a robust auditable trail of how identities were proven. This in turn may help to obtain credit at a more attractive interest rate.

E-invoicing
The development of a digital identity could enhance e-invoicing. Invoices serve several purposes including crystallising a tax event and communicating a debt, along with instructions on how to settle the debt. Tax authorities in a number of jurisdictions now use digital identities embedded in electronic invoices to quickly learn about taxable events and later use this to ensure that the correct taxes are remitted. Payment diversion fraud is one of the largest single areas of fraud in the world, digital identities embedded in invoices could be used to identify fraudulent invoices that include incorrect payment details (e.g. a fraudster's bank account) and help reduce this significant cost to the nation.

Prioritisation

Individuals and businesses will adopt a digital identity system only if it provides value and engenders trust. Government led communication, partnering with industry, on the guarantees within the Digital Identity Trust Framework will be crucial, along with robust governance, commitment to privacy and cybersecurity from the outset. To facilitate its widespread adoption, it needs to be easy to set up and easy to use, and its networks must be integrated and interoperable across the economy.

Relevant legislative, technological and international developments

The UK has an opportunity to lead the way in introducing a digital identity standard that is widely adopted across sectors. The success of the digital identity is linked to its interoperability and ability to respond to the needs of individual, private sector and public users. The wide adoption and success of a digital identity will hinge on its ability to accelerate and link up to different industry and government initiatives as well as keep pace with international developments. In this regard, Sage believes the below initiatives and case studies should be taken into consideration:

- **Open Banking –** Alignment should be sought with the Bank of England's Open Banking Initiative which requires banks to share customer information with third-party providers, with customer consent. Similarly, wide adoption and acceptance will require clarity on consent, security, privacy and accountability, while enabling a more streamlined and inclusive experience.

- **UK National Data Strategy –** Alignment should be sought with objectives and principles of the UK National Data Strategy to be a world leader in data, whilst protecting individuals, supporting innovators and entrepreneurs, building trust and confidence in data use and removing existing barriers.

- **UK Digital Strategy –** Alignment should be sought with the new UK Digital Strategy with an emphasis on its objectives of creating a highly skilled and digital workforce, building world class digital infrastructure and securing alignment with the EU.

- **EIDAS –** The eIDAS regulation has been adopted by the EU with the purpose of simplifying cross-border use of electronic services and supporting a common digital market. It aims to reinforce compliance with GDRP and Privacy by Design as well as align with other EU-wide initiatives like PSD2 and the Anti-Money Laundering Directive.

- **Estonia E-Identity –** In Estonia, the state issues a digital identity, which in addition to serving as the national photo identity card, enables access to e-services including, I-voting, national health services, verification for online banking, digital signatures and travel within the EU. There is a 98 percent up take by citizens.

- **World Economic Forum Platform for Good Digital Identity/Identities Coalition Network –** Established in 2018 in Davos, the Identities Coalition Network seeks to advance global activities that are collaborative and develop guidance that will put user interest at the centre. Its principles promote a fit for purpose, inclusive, useful, and secure application of a digital identity framework.

- **G20 Digital Identity Framework –** In 2018 under the auspices of the Argentinian Presidency of the G20, the recommendation for a digital identity framework was proposed to help harness digitization and promote financial inclusions for individuals and SMEs. In 2020 this remains a priority under the Saudi Arabian presidency with a focus on interoperability and compliance in international trade.

Leadership and collaboration

Leadership

While there are multiple government departments for which identity is important to their operation (e.g HPMO, ICO, DCMS, FCA, HMRC) the government should nominate one single point of contact as the lead on digital identity. In this case, Sage believes that ICO would be best positioned.

Collaboration

While one government entity should take the lead, they must act as the convener and pursue close collaboration with all relevant government stakeholders as well representatives across industry. Private-public collaboration is essential for the broad uptake and application of a digital identity. Businesses can innovate processes that could leverage digital identity to boost efficiency, improve customer experience, work to facilitate the development of global standards, and collaborate with governments to conduct bespoke cost-benefit analysis of digital identity and develop new digital identity programs. A cross industry group that aligns closely with government and regulators, like the Open Banking Implementation Entity, is needed. In addition, collaboration should also be sought with international organisations and standard bodies to enhance international operability and help to position UK as a leader in this area.

Conclusion

Sage supports the adoption of a digital identity framework that can apply across all sectors and work for both individuals and businesses. Sage looks forward to the opportunity to further collaborate with DCMS on helping to make the digital identity a reality.