Rt Hon Peter Kyle MP
House of Commons
London
SWQ1A 0AA

23rd July, 2024

Dear Mr Kyle,

The UK must evolve and accelerate its current Digital ID strategy. The UK Digital Identity and Attributes Trust Framework (DIATF) is a solid start which can built upon to put the UK in a leading position on digital trust.

Over time, digital ID will become the core component of a critical global digital infrastructure and it therefore needs a cogent long-term UK government plan. It will also be a foundational element if the UK wishes to enable domestic and international trade and be perceived as an advanced technological nation.

A digital ID allows a person or business to prove who they are, that they are real and what they are eligible to do, through a low-friction process across a broad range of use cases. With a digital ID, both face-to-face and online services can be accessed instantly and securely. Digital ID can also be used to assess eligibility criteria, such as age appropriateness or qualification-based job requirements. Once an individual has been onboarded by means of their digital ID, they are able to reuse it to access and manage their account on an ongoing basis with that service provider.

Digital ID can unlock significant value to the UK economy. McKinsey states that the benefit of digital ID to countries like the UK, Brazil, China, Ethiopia, India, Nigeria and the United States could be equivalent to between 3% to 13% of GDP by 2030. The overall value, however, goes beyond GDP, benefiting individuals, business services and citizen-facing government departments alike when it comes to inclusion, fraud prevention and promoting data privacy.

The UK is already starting to see the benefits of digital ID in areas such as right to work and right to rent checks. Over 30% in time-saving has been quoted by some employers through using digital ID to check for right to work.

A 2023 public dialog run by the Department for Science Innovation and Technology (DSIT) identified that citizens consider that digital ID should be for public benefit and should be accessible to anyone who would wish to use it, regardless of their background. Digital inclusion will therefore also be improved by ensuring all citizens who want a digital ID are able to obtain one.

The following actions should be undertaken to evolve the current Digital ID strategy:

1. Evolve the DIATF to include a digital wallet strategy for the UK

There is rapidly increasing and more frequent use of digital wallets across the world and the UK should take a leading approach in this emerging trend.

Digital wallets allow a user to hold digital versions of their credentials. They provide users with convenience for making payments and increasingly (re)sharing their personal information with accepting parties.

As part of a UK digital wallet strategy, we encourage government departments and private companies to create and issue digital credentials that can sit within a user's digital wallet, such as proof of education, employment qualifications, DBS screening results and visas/travel documents. This will catalyse the digital economy and promote new commercial models for all parties involved.

Common proof of identity documents such as driving licenses and UK passports should have equivalent digitalised versions and be afforded the same legal status as their physical ID forms.

Relevant sector-based regulations and associated published regulatory guidance should be updated to accommodate acceptance of digital IDs and digital credentials. It is of fundamental importance that regulatory barriers (or the perception thereof) to the acceptance of digital IDs and digital credentials are removed to promote not only growth but security for the UK's regulated sectors.

The government must support the emergence of new digital wallet ecosystems. This means allowing the private sector to deliver digital ID through digital wallets within government guidelines and allowing DIATF certified digital wallet providers to hold and present government-issued digital credentials whilst ensuring that these credentials are properly and securely managed. If Apple and Google wish to carry these credentials in their wallets, they must be certified accordingly and must comply with the restrictions on use demanded by the DIATF.

The provision and maintenance of digital wallets should be left to the private sector, which is better placed to innovate and keep up to date with the latest anti-fraud technology. The private sector is more likely to commit to ongoing innovation, improving cost effectiveness and technical evolution in a way that a government delivered wallet would not be able to match. This will lead to a competitive market for digital ID and digital wallet providers.

The provision of any government wallet to manage digital ID and credentials is likely to raise privacy concerns for citizens and fears that the government is monitoring their actions through usage of its wallet, especially if the wallet is used for private sector transactions. Several EU countries are realizing this as they progress to implement EUDI Wallets and are seeking private sector wallet providers to deliver their EUDI Wallet obligations, including Germany, Spain, Italy, Sweden and Estonia.

The DIATF must make it very clear that digital ID is not the same thing as a national ID or a national database of IDs. Digital IDs will be delivered by a range of DIATF-certified private sector providers, who themselves distribute each user's data in both a secure and privacy preserving way that is in sole control of that user. This is a diametrically opposite approach to a national ID scheme and is a better means to achieve identity trust through rules and certification, not data centralisation or government oversight.

UKAS accredited certification bodies who certify digital wallet providers to the DIATF must therefore robustly scrutinize that wallet providers have implemented appropriate designs for data privacy and security of data in such a way that personal information is still protected if the user's mobile device is stolen.

The DIATF must allow for UK digital wallet interoperability with European Union Digital Identity (EUDI) wallets. From a technical and legislative perspective, the EU is following a 'decentralised' digital wallet route, where the information in the wallet is held remotely for each user rather than in a centralised database. We believe that this is a sensible approach for managing users' data privacy.

We encourage the UK government to set out, publish, and pursue a digital ID inclusion strategy. This is to ensure that population-wide inclusion is achieved. We believe this can be achieved through the recognition of a digital vouching system.

2. UK public / private sector positioning

GOV.UK One Login should not be made available as a digital ID for access to private sector services. Government should not compete with the private sector market of digital wallet providers that it is looking to enable. A clearly stated position on this will mean investment decisions on digital ID for the private sector can be made with confidence, resulting in a vibrant and innovative private sector market for digital ID.

Permit a GOV.UK One Login (that has achieved a certain level of confidence) to be used as identity evidence for creating private sector digital IDs under the DIATF. This will aid inclusion by enabling users who have already attained trust through the process of accessing government services, to share this trust with a private sector digital ID provider of their choice. The UK guidance for ID proofing (GPG45) already allows EU member state electronic IDs to be used as ID evidence, so the guidance should be extended to include UK government electronic IDs (i.e. GOV.UK One Login) as well.

Permit access to government services via suitably DIATF-certified private sector digital IDs, allowing citizens to choose a non-government ID provider if they wish to do so.

Permit access to government data for the purposes of identity proofing and eligibility, as would have been enabled through the Digital Verification Services section of the Data Protection and Digital Information Bill. Focus on data sets that will improve inclusion in the digital ID ecosystem and that will prove eligibility for services, such as proof of income.

3. Lead on cross-border interoperability

We believe that the UK should drive and coordinate the ongoing international work for cross-border interoperability of digital wallets (ie. digital IDs and digital credentials). This could be done by supporting the Open Identity Exchange and our affiliates to agree and design open approaches and standards to enable interoperability and enabling non-domestic ease of access to UK businesses, products and services, thereby empowering UK trade with other nations.

Direct UK government support for a robust interoperable digital wallet system will signal to the world that the UK is at the forefront of technological advancement. It will attract international partnerships, foster trade relations, and enhance the UK's global influence.

In summary, the current UK DIATF is an excellent start but needs to evolve further and at a faster pace to embrace growing use of digital wallets and prepare for international interoperability. Addressing the points stated above will provide citizens and businesses with online trust, enabling significant economic growth and showcasing UK technical thought leadership across the globe. UK businesses will be able to export services around the globe easily and with trust.

Your sincerely,

Gareth Narinesingh

Identity Development Director
Open Identity Exchange