Law Society of Scotland

Survey Response

UK Government: The UK digital identity and attributes trust framework – Trust framework alpha survey

March 2021

Introduction

The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors and 600 Accredited Paralegals.

We are a regulator that sets and enforces standards for the solicitor profession which helps people in need and supports business in Scotland, the UK and overseas. We support solicitors and drive change to ensure Scotland has a strong, successful and diverse legal profession. We represent our members and wider society when speaking out on human rights and the rule of law. We also seek to influence changes to legislation and the operation of our justice system as part of our work towards a fairer and more just society.

Our Technology Law and Practice Committee and our Privacy Sub-Committee welcomes the opportunity to consider and respond to the UK Government's Trust framework alpha survey: The UK digital identity and attributes trust framework. We have the following comments to put forward for consideration.

Question 1: Do you agree with our trust framework approach for digital identity?

We agree in principle with the trust framework approach for digital identity. Any trust framework system should be technology neutral, transparent and have the appropriate controls in place to ensure that users are comfortable in using the system. To be effective this would have to be a fair and highly trusted system which delivers robust authentication and is accessible to all.

We note that you anticipate different levels of digital identity. Users would need to be aware of what data they were sharing with particular providers. It must therefore be made clear to users what level of data is required for that purpose to facilitate the correct amount of data sharing.

It is also important to address liability and insurance issues and to have clarity on who would be liable for any failures in the system. For example, if there is a data breach of an individual's data, who would be liable for that breach?

It is of critical importance that the original creation of a digital ID can only be achieved in relation to a real and recognised person and that a third party is able to rely on it.

Question 2: Do you agree with our open policy making approach of releasing an alpha document?

We agree with your open policy making approach of releasing an alpha document. Even once the framework has been finalised, it will be important to review it regularly and make any necessary adjustments.

Question 3: Which of the areas outlined in the survey should we prioritise developing in trust framework requirements?

All of the elements outlined in the paper are required if the Trust Framework is to function properly. Without technical interoperability, the framework will not function but other elements, such as identity standards and privacy and data protection are essential to create trust. One of the core principles for building systems is that they comply with modern data protection and privacy legislation. In the same way, we consider that inclusion should be one of the key considerations in the way that the Trust Framework is built. This will require organisations to understand the demographics of their users to assess what is needed. At the same time, inclusion should be considered in a wider context to ensure that those who are not able, or do not wish, to utilise digital identities, are able to continue accessing services and participating in society.

Furthermore, the framework is likely to need to be adjusted over time so that it continues to deliver and improve upon its credentials in terms of fraud management, privacy and data protection and inclusion.

Question 4: To what extent do you agree that the requirement to submit an annual exclusion report will help to hold companies accountable to be more inclusive? (Strongly disagree, disagree, neutral, agree, strongly agree)

Neutral.

We are unable to provide a detailed response here as it is not clear from the paper as to what information should be included in the exclusion report and specifically what companies are being asked to measure by compiling such a report.

Question 5: To what extent do you agree that companies will be happy to produce an exclusion report? (Strongly disagree, disagree, neutral, agree, strongly agree)

Neutral.

It may be that companies would be happy to produce an exclusion report as they are used to reporting on other matters, for example, Equal Pay. As a generality, businesses may be wary about reporting due to privacy risks. However, for the same reasons outlined at question 4 above we are unable to provide a detailed response.

Question 6: To what extent do you agree that the trust framework will make it easier for people without traditional identity documents to access an online service? (Strongly disagree, disagree, neutral, agree, strongly agree)

Neutral.

It is difficult to see at this stage how the trust framework would make it easier for people without traditional identity documents (e.g. passports) to access some services, for example, banking services. It would assist if there was further information available as to how Government services may fit into this framework and how those services would be offered without the suggested trust framework.

Question 7: What additional inclusion requirements should be included in the trust framework?

It is difficult at this stage to determine any additional requirements. We believe, however, that there could be a risk that this becomes omnipresent and therefore some people could unintentionally be excluded from accessing services.

Question 8: To what extent do you agree that the counter fraud and security measures will ensure best practice is upheld by trust framework members? (Strongly disagree, disagree, neutral, agree, strongly agree)

Neutral.

We believe that the measures and controls as outlined in the paper appear to be aligned with existing legal and regulatory frameworks.

Question 9: What additional counter fraud or security requirements should be included in the trust framework?

We as a regulator and Anti-Money Laundering (AML) supervisor have an interest in the prevention of financial crime. We consider that the proposed framework has the potential of driving efficiencies in AML and onboarding from a consumer and firm perspective, which we believe would be supported by other AML supervisors. Should the proposal be to allow regulated persons to "rely on" ID Providers under the terms of Regulation 39 of the Money Laundering Regulations[1], the regulations would require to be amended to ensure that ID Providers were brought into scope of the regulations and appropriately supervised. Otherwise another legal mechanism would need to be established to allow such regulated persons to be able to use ID Providers for the purposes of AML-related due diligence.

We note that greater collection of data in terms of authentication, may also create a greater risk of threat to privacy and infringement of data protection rights if the data/details of a person's attributes are lost or stolen. It is therefore important to strike a balance between creating trust by securely identifying individuals, while at the same time collecting only the data that is really necessary to achieve this objective. Organisations should only be able to access those attributes which are necessary for the purposes of providing the service in question.

Question 10: To what extent do you agree that the trust framework facilitates interoperability, as defined by the ability to use a digital identity created in one context in another? (Strongly disagree, disagree, neutral, agree, strongly agree)

Disagree.

There is an essential level of technical interoperability in which a system has to function. There could be concerns in using a trust profile in a low-risk situation as authentication in a higher risk scenario. Further analysis is required to assess to what extent this is a risk and controls put in place as appropriate.

[1] https://www.legislation.gov.uk/uksi/2017/692/regulation/39/made

Question 11: In order to facilitate interoperability, do you think that the trust framework should: Mandate technical specifications, recommend technical specifications, make no reference to technical specifications

It is important to have standards in terms of technical specifications to make it easier for those wishing to use the service to achieve these standards. It is fundamental that there is flexibility to encourage innovation and allow access for all businesses within the appropriate sectors, for example, SMEs. We suggest that the framework should seek to endorse existing technical specifications so far as possible (for example, utilising the frameworks set out in the eIDAS Regulation[2]). This avoids duplication of standards and reduces the barrier to entry. We consider it likely that agencies will require a Qualified Electronic Signature (QES) as standard and therefore it would be sensible to have the same approach to avoid multiple identification verification processes.

Question 12: To what extent do you agree that the trust framework provides enough protection for users on use of their data? (Strongly disagree, disagree, neutral, agree, strongly agree)

Neutral

We strongly agree that the trust framework should accord with privacy and data protection legislation. The Data Protection Act 2018 and GDPR set high standards for robust data protection. However, the trust framework may need to give greater guidance – for example around processes and cybersecurity protections – to ensure that the overarching framework guarantees protection. Furthermore, the standards will need to be enforced if the TF is to deliver the benefits while safeguarding user data.

Question 13: Are there any obligations or requirements which may harm the interests of users?

We do not anticipate that the obligations or requirements set out in the framework would harm the interests of users, subject to implementation as discussed in our answers above.

[2] As incorporated into UK law under the European Union (Withdrawal) Act 2018 - https://www.legislation.gov.uk/ukpga/2018/16/contents/enacted

Question 14: Are there any obligations or requirements which may make digital identity impossible to implement for your organisation?

We do not anticipate that any reasonable obligations or requirement would make digital identity impossible to implement for our organisation. However, further detail as to the practical implementation of the framework is necessary to provide a more definite response.

Question 15: Do you want to provide line by line feedback on the UK digital identity and attributes trust framework?

We are keen to support the creation of a practical and proportionate digital identity and attributes trust framework. This touches upon a number of issues of importance to the Law Society and its members. This includes the importance of creating an inclusive framework, its role in preventing fraud, our inherent interest as an AML supervisor, the importance of ensuring privacy and data protection, and the position of the UK as a modern digital economy. We would be very pleased to arrange for further engagement to discuss the trust framework when more specific proposals have been published.

Law Society of Scotland

For further information, please contact:
Gillian Alexander
Professional Practice Team
Law Society of Scotland
gillianalexander@lawscot.org.uk