A consultation on digital identity and the governing body which will oversee the rules on digital identity

Department for Digital, Culture, Media & Sport

Response from the Emerging Payments Association

September 2021

Introduction

The Emerging Payments Association (EPA) welcomes the opportunity to contribute to the Consultation on "Digital identity and the governing body which will oversee the rules on digital identity" published by the Department for Digital, Culture, Media & Sport in August 2021.

The community's response contained in this paper reflects views expressed by our members and industry experts recommended by them. As the EPA's membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been co-ordinated by Jane Jee, Chair at Kompli-Global Ltd and Project Lead of the EPA's Project Financial Crime. We would also like to express our thanks to the named contributors below, and the team at the Department for Digital, Culture, Media & Sport for their continuing openness in these discussions:

- Jane Jee - Chair - Kompli Global
- Steve Pannifer - Digital Identity Subject Matter expert - Consult Hyperion
- Jonathan Jensen - Regulatory Policy Advisor - GBG plc
- Andrew Churchill - Author - Digital Identification and Standardisation BSI PAS499

We hope this contribution advances our collective efforts to ensure that the UK's payments industry continues to be progressive, world-leading and secure, and effective at serving the needs of everyone who pays and gets paid.

Tony Craddock
Director General
Emerging Payments Association

CREATING A DIGITAL IDENTITY GOVERNANCE FRAMEWORK

1. Do you agree an existing regulator is best placed to house digital identity governance, or should a new body be created?

- The EPA considers that there is no appropriate existing regulator and that a new body should be created to house digital identity governance.
- The regulator and governing body should be directed to ensure that all measures adopted actively prevent financial crime, rather than just seek 'compliance', and be judged primarily on this metric.
- Alongside existing legal requirements, such as for a Privacy Impact Assessment, a Financial Crime & Security Impact Assessment should be required for any measures being adopted that might aid and abet international organised crime.
- Given the set-up costs and time required to establish a new regulator, the alternative would be to create a new division in an existing regulator, but this is regarded as sub-optimal. If an existing regulator is chosen, the strongest candidates appear to be:
    - The ICO, given the close relationship between digital identity and privacy. However, the ICO has little experience and expertise in the significance of digital identities in preventing financial crime, which includes fraud. Some compromises on privacy may be needed if we are to make better inroads in this area.
    - The CMA, given its role in shaping the industry's approach to open banking. Open banking and future open API initiatives are closely related to, and may well overlap with, digital identity initiatives.

2. Which regulator do you think should house digital identity governance?

The EPA considers that none of the existing regulators are wholly appropriate and that a new and independent regulator and a new governing body would be the best option. Whichever regulator takes on the responsibility they should have a number of characteristics. The new regulator should have a pro-innovation, pan-economy, cross-sector approach and have expertise in:

- Digital identity mechanisms in the UK and internationally
- Data science
- Developing markets
- The significance of digital identity both in relation to privacy and in the context of preventing financial crime

3. What is your opinion on the governance functions we have identified as being required: is anything missed or not needed, in your view?

Individual organisation versus scheme oversight needs greater clarity. We envisage that suppliers will want to maximise their market opportunity by being part of multiple schemes as well as being recognised directly by the governing body. Depending upon how oversight arrangements work, this could lead to a lot of duplication of effort or a lack of clarity over who is responsible to oversee what.

4. What is your opinion on the governing body owning the trust framework as outlined, and does the identity of the governing body affect your opinion?

The EPA considers that it is beneficial for the governing body to own the Trust Framework and have responsibility for the update process. It is essential that the governing body has access to expertise to

help understand the evolving digital identity landscape both in the UK and globally and from all angles – business, legal and technical. It is unlikely this expertise is present in any current regulator to the extent that would be needed to inform the future development of the framework. The governing body could be shaped as a collaboration between the private sector and the Government, in the form of an elected board with a limited mandate and checks and balances in place.

5. Is there any other guidance that you propose could be incorporated into the trust framework?

Since there are multiple approaches to digital identity in the market, the framework should be outcome based – stating what digital identity should deliver (e.g. assurance in identity, reduction in fraud etc) - but not be prescriptive as to how to do it. As currently written, the framework is not outcome based. It aligns too closely to a particular approach to digital identity, namely federated identity service provider-based identity. Whilst the framework says it will support other approaches (e.g. SSI) it is not apparent how this will be achieved.

6. How do we fairly represent the interests of civil society and public and private sectors when refreshing trust framework requirements?

The consultation suggests that advisory groups will be set up to inform the governing body. It is essential that those advisory groups ensure that the voices of all stakeholders are heard. A potential danger with advisory groups is that their advice is not heeded, or they feel that their advice is not heeded – leading to the credibility of the governing body being reduced. The government should consider appointing representatives from all stakeholder groups to the governing body itself to ensure real representation in decision making, as opposed to more 'arm's length' collaboration. In particular smaller, innovative private companies' views should be considered.

7. Are there any other advisory groups that should be set up in addition to those suggested?

In addition to those listed, the governing body should seek to engage with relying parties (i.e. the buyers of digital identity services). The governing body should also seek to identify qualified independent experts who do not come with a specific agenda.

ACCREDITATION & CERTIFICATION

8. How should the government ensure that any fees do not become a barrier to entry for organisations while maintaining value for money for the taxpayer?

Fees must be set to maximise the chances of the framework succeeding. If fees are to be set from day one they should be based on the intended target state, such as a projection on the number of framework members in a mature ecosystem. This will mean that the governing body will need to rely on taxpayer funding more heavily at the beginning. Any fees should be set so as not to be prohibitive to new entrants. Where members derive significant value from their membership of the scheme, then a fee will be more palatable.

OVERSIGHT/MANAGEMENT OF ORGANISATIONS/SCHEMES

9. Do you agree with this two-layered approach to oversight where oversight is provided by the governing body and scheme owners?

Yes, as this will allow the governing body to be more hands-off and make the ecosystem more scalable. There are however two issues that needs to be carefully considered:

- Having both scheme and direct oversight of members could result in duplication of effort and confusion or conflicts.
- If there is a proliferation of schemes this will result in a very complex environment, again resulting in duplication of effort and placing a significant burden on providers wishing to participate across all schemes.

10. Do you agree the governing body should be an escalation point for complaints which cannot be resolved at organisational or scheme level?

Yes, a single escalation point is essential to resolve disputes. However, the criteria for such escalation, the process the governing body follows and the potential actions that can be taken by the governing body will need to be clearly defined.

11. Do you think there needs to be additional redress routes for consumers using products under the trust framework?

If yes, which one or more of the following?:

a. an ombudsman service

b. industry-led dispute resolution mechanism (encouraged or mandated)

c. set contract terms between organisations and consumers

d. something else

If no, do you think the governing body should reserve the right to impose an additional route once the ecosystem is more fully developed?

It is realistic to expect schemes to provide dispute resolution within the scope of their schemes. This is what happens in payment networks today. Set contract terms (which consumers will not read or understand) by itself is unlikely to be effective. The support of an ombudsman service will help.

12. Do you see any challenges to this approach of signposting to existing redress pathways?

The goal should be that it is clear to individuals and organisations from which they seek redress and why. The example cited is important because digital identity and data protection are so closely connected. In some cases, it may be difficult to distinguish a data protection failing in a digital identity service from some other failing in the service.

13. How should we enhance the 'right to rectification' for trust framework products and services?

A "no wrong door" policy could place a significant burden on framework participants. What is involved in identity repair will depend on the type of digital identity system in question. In a federated system the person will be likely to have a primary relationship with an Identity Provider – and it may be reasonable to expect an Identity Provider to assist with identity repair. In a decentralised system however, identity repair may require credentials to be re-issued from different sources. Furthermore, the secure wallet provider would have no visibility of the contents of the wallet (and nor should they).

14. Should the governing body be granted any of the following additional enforcement powers where there is non-compliance to trust framework requirements?

a. Monetary fines

b. Enforced compensation payments to affected consumers

c. Restricting processing and/or provision of digital identity services

d. Issue reprimand notices for minor offences with persistent reprimands requiring further investigation

All the above enforcement powers should be granted. Enforcement powers should be vested in both the regulator and the governing body so that the appropriate body can take action depending on the nature of the breach. Sanctions should be commensurate with the severity of the breach but should also not be a barrier to market entry.

Notwithstanding the above, the government should encourage providers to join the framework, especially whilst the market is still nascent. The threat of monetary fines and enforced compensation may act as inhibitors. As with data protection, this may be something that can be revisited as the market grows and the risks are better understood. Restricting processing and reprimand notices are softer controls and therefore likely to be more appropriate to start with.

15. Should the governing body publish all enforcement action undertaken for transparency and consumer awareness?

We agree that this is appropriate.

16. What framework-level fraud and security management initiatives should be put in place?

Framework- level fraud and security management initiatives must be flexible so they can adapted to evolving fraud typologies. Identities should be assessed for fraud with scheme flexibility to support behavioural, digital and biometric fraud. The EPA also encourages DCMS to consider the Financial Action Task Force (FATF) Guidelines on Customer Due Diligence (CDD), which takes a comprehensive approach to protecting against both fraud and security, as well as bolstering system integrity (protecting against money laundering and terrorist financing). The OIX's Fraud Guidelines are also a useful resource for digital identity more broadly: https://openidentityexchange.org/networks/87/item.html?id=453

17. How else can we encourage more inclusive digital identities?

Scheme operators should be encouraged to ensure they have a wide range of identity providers who in turn offer a range of identity proofing methods.

Creating digital identities requires robust identity proofing using trusted datasets. Opening access to HMG datasets, e.g. HMRC, DWP, Passport Office and the DVLA, would assist in that process, especially where individuals have limited data available within the private sector.

18. What are the advantages and disadvantages with this exclusion report approach?

The report should be called an Inclusion Report in order to focus on the inclusive nature of its purpose. The report should state who is included but cannot state who is excluded because by definition, as they are excluded, the service provider will not know who they are.

There are negative connotations with the term exclusion which could harm the reputation of a service provider in an unwarranted way. Exclusion should be identified at the Trust Framework level.

Inclusion obligations should only apply to consumer facing participating organisations. Inclusion reporting should include the context of inclusion, e.g. any requirements that need to be met to be a customer of an identity provider.

19. What would you expect the exclusion report to include?

It is difficult to provide comment at this time, however there is a risk that exclusion reports could become a source of information for criminals to garner what firms look for when identifying fraud.

ENABLING A LEGAL GATEWAY BETWEEN PUBLIC AND PRIVATE SECTOR ORGANISATIONS FOR DATA CHECKING

20. Should membership of the trust framework be a prerequisite for an organisation to make eligibility or identity checks against government-held data?

No. The EPA considers that this is an unnecessary commercial restriction. Government held data should be available to all approved organisations. Some use cases will be outside the Trust Framework, e.g. driving entitlement or benefits status.

It is crucial for the UK's digital economy to maximise the use of government data attributes. Other methods of identity verification should not be disadvantaged by an inability to access HMG data. Mandating membership would impact inclusion negatively.

21. Should a requirement to allow an alternative pathway for those who fail a digital check be set out in legislation or by the governing body in standards?

We recommend that alternative pathways should be left to the governing body.

22. Should disclosure be restricted to a "yes/no'' answer or should we allow more detailed responses if appropriate?

For identity verification, a yes / no response may be appropriate. However yes / no can cause issues, e.g. with name and address variations. An individual should be able to authorise sharing of actual identity attributes.

In some use cases, attribute data is always required, e.g. driving licence entitlements (DVLA) or income verification (HMRC).

A self-sovereign identity model would allow an individual to hold their HMG identity credentials in a digital wallet and consent to share them on a case-by-case basis (similar to the EU digital identity wallet).

23. Would a code of practice be helpful to ensure officials and organisations understand how to correctly check information?

At a technical level there should be clear documentation and Codes of Practice for accessing APIs, in line with the UK Government Technology Code of Practice. For wider handling and check of identity information a Code of Practice would help drive alignment across industries and therefore would be beneficial.

24. What are the advantages or disadvantages of allowing the onward transfer of government-confirmed attributes, as set out?

Allowing onward transfer could enable third parties to build digital ID services which use the data (Identify Providers) for relying parties. However, such relying parties may then not be certified and there is a risk of poor behaviour undermining trust across the whole system. Hence, we believe that establishing criteria for the certification of third parties working with government confirmed attributes will be essential to build trust in the ecosystem.

The EPA understands that not all data should be treated identically depending upon the requirements of their use. If firms are handling more sensitive information, they should face greater scrutiny than those handling yes/no attributes.

ESTABLISHING THE VALIDITY OF DIGITAL IDENTITIES AND ATTRIBUTES

25. Would it be helpful to affirm in legislation that digital identities and digital attributes can be as valid as physical forms of identification, or traditional identity documents?

Legislation to confirm digital identities and attributes are as valid as physical identity documents would be a significant boost to the digital economy and underpinning digital identity with legislation would increase confidence in digital identity and promote its widespread adoption.

A digital identity's equivalence to a physical identity document would be subject to the GPG 45 level of confidence it had been assured to. A digitised passport or driving licence should be seen as legally equivalent to a physical version. In the absence of malpractice or negligence, digital identity providers

should not be held liable for falsely obtained digital identities, in the same way as HMG is not held liable for falsely obtained genuine passports or driving licences today.

About the EPA

The Emerging Payments Association (EPA), established in 2008, sets out to make payments work for everyone. To achieve this, it runs a comprehensive programme of activities for members with guidance from an independent Advisory Board of 16 payments CEOs.

These activities include a programme of digital and (when possible) face-to-face events including an online annual conference and broadcast awards dinner, numerous briefings and webinars, CEO Round Tables, and networking and training activities. The EPA also runs six stakeholder working groups. More than 100 volunteers collaborate on the important challenges facing our industry today, such as financial inclusion, recovering from Covid-19, financial crime, regulation, access to banking and promoting the UK globally. The EPA also produces research papers and reports to shed light on the big issues of the day and works closely with industry stakeholders such as the Bank of England, DCMS, FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, UK Finance and Innovate Finance.

The EPA has over 150 members that employ over 300,000 staff and process more than £7tn annually. Its members come from across the payments value chain including payments schemes, banks and issuers, merchant acquirers, PSPs, retailers, TPPs and more. These companies have come together to join our community, collaborate, and speak with a unified voice.

The EPA collaborates with its licensees at EPA EU and EPA Asia to create an interconnected global network of people passionate about making payments work for all.

See www.emergingpayments.org for more information. Contact malik.smith@emergingpayments.org for assistance.