##

**Digital Identity: Call for Evidence**

|  |  |
| --- | --- |
| Name | Beth Rudolf |
| Organisation | Conveyancing Association |
| Job title | Director for Delivery |
| Address | c/o Maxwell Chambers, Newport |
| E-mail  | brudolf@conveyancingassociation.org.uk |
| Telephone | 07814 358627 |

The Conveyancing Association is a trade association representing ‘serious conveyancers’ across England and Wales. We have 75 members who together deal with 30% of the transactions for value recorded at HM Land Registry.

Our aim is to improve the home moving process for the consumer.

## Questions

## **Questions on 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?

Yes. In the conveyancing process there are multiple parties who need to check that they are dealing with the person with whom they believe they are dealing and that that person is entitled to the identity which they have presented and that they, in the case of a seller, are the true owner of the property being sold. This is vital in avoiding fraud and a key gap in the current process which allows significant frauds to be perpetrated and increases professional indemnity insurance premiums and therefore the cost of provision of services to the customer.

Up until now organisations have been reliant on copies of identity documents being ‘certified as a true copy of the original and a true likeness of the individual’. There is nothing to evidence that that certification itself is genuine other than costly investigative activities which may be ineffectual as the person providing the certification is unlikely to keep records. [Dreamvar (UK) Ltd v Mischon de Reya and others; [2018] EWCA Civ 1082].

Employers may also be able to use, in appropriate circumstances, digital identity to flag up potential issues, for example in the employment of individuals with criminal records to positions unsuitable for people with a history of these offences.

What other ideas or options would help?

The wider use of biometric data to confirm identity and the publishing of standards on what is acceptable through regulators and government departments. Currently, the obligations are either outcome based or unclear as to whether digital solutions can be employed. This leads to regulated professionals relying on paper copies of documents

If the regulators such as Council for Licensed Conveyancers, Solicitors Regulatory Authority, CILEx Regulation, along with government departments such as HMRC and HM Land Registry set clear standards as to what is acceptable and were explicit as to when conveyancers can rely on and share digital identity solutions then there could be greater uptake and the industry and the consumer would benefit.

1. 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?

It is necessary to verify your identity and source of funds and wealth to a variety of stakeholders in the home moving process. Delays and frustration occur if you are required to present your identity documents to multiple different parties or pay for certification of those documents and they all have different requirements for different forms of verification.

Professionals in the process are concerned about their ability to rely on another stakeholder’s identity verification processes, especially if outsourced services are involved or they could incur additional liabilities if they allow others to rely on their own know your customer checks. This prevents the use of one source of truth in the identity verification process across the transaction.

For a legitimate home mover this can make little or no sense. For a fraudster, they can take advantage of the gaps in verification between parties.

Seller identification fraud is particularly impactful on buyers where they pay over the purchase price to someone posing as the seller only for HM Land Registry to refuse to register their title because they have uncovered a fraud.

The fraudsters focus on high value assets and in several cases over a million pounds have been lost in property transactions.

Similarly for buyers transferring money for the purchase, there are significant risks where they are unable to confirm the identity of the account to which they are sending the funds. Media reports indicate that up to £600,000 have been lost in any one transaction where the criminal has been successful in diverting cash to a different account which they control.

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

See above. Each stakeholder has different needs and requirements based on their own assessment of risk and practices and a home mover may have to pay between £10 and £20 for the services used by each them to verify their identity.

Failure to identify seller ID fraud has resulted in increased insurance premiums across the market and therefore cost of services to the home mover.

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

Even someone with a thin file will have a digital footprint where they have accessed services or someone has accessed them on their behalf. The current process to obtain an official document sets out what data is necessary to establish to the relevant authority that you are entitled to the document eg to obtain a passport or drivers licence. It should therefore be possible for the majority of people using a combination of available data such as passport, citizenship certificate, National Insurance number, and verification from professionals who have interacted with them, in the same way as used to be necessary for passport applications.

Whilst it may be more bothersome for those whose lives have been conducted without digital services, these will become fewer and fewer as time goes by and the establishing of a digital is a one off process compared to the current multiple occurrence of a need to prove an attribute through their lives. There might need to be transitional arrangements for certain citizens in particular circumstances but these should not inhibit the general introduction of digital processes.

1. What currently prevents organisations from meeting the needs stated above?
* Lack of clarity of the acceptability of digital solutions.
* Lack of standard approaches to what constitutes an acceptable digital solution
* Perception or mis-perception of requirements from lenders and regulators.
* Fear from practitioners of additional costs making their service uncompetitive.
* Fear of additional liability being created where verification activities are shared.
* Fear of the unknown and the lack of recognisable standards to provide reassurance.
1. Where do you see opportunities for a reusable digital identity to add value to services? Could you provide examples?

In the home moving process it would be hugely beneficial to have one source of truth when considering the evidence of identity which could be shared between stakeholders.

In the worst case scenario, as a home mover buying and selling property, you may be required to prove your identity to:-

* The estate agent selling your existing property
* The conveyancer acting on your sale
* The estate agent selling your new property
* The broker organising your mortgage
* Your new lender
* The conveyancer acting on your purchase
* The conveyancer acting for the new lender
* The Land Registry

There is no guarantee that any of those parties will require the same information.

There are particular issues in proving that the person whom you are dealing with is the registered owner of the property at HM Land Registry, which has resulted in multiple million pound fraud being committed in the past.

By enabling a verified and authenticated multi-faceted digital identity which can be shared between stakeholders the consumer experience can be improved, costs can be reduced and fraud can be eradicated.

## **Questions on criteria for trust**

1. What are the building blocks essential to creating this trust?

These have been thoroughly detailed in the call for evidence. Overall, for trust to exist in a regulated industry, stakeholders need to be comfortable that they have regulatory approval to utilise a digital identity for the stated purposes and that there is a state approved identity standard which can be demonstrably adhered to. There needs to be a clear route to resolving any disputes which may arise.

1. How does assurance and certification help build trust?

Regulated and insured entities need to be confident that they are not increasing their liability by relying on a particular digital solution. Appropriately certified products or standards enable their insurers to agree an approved standard which, if met, will reduce fraud, claims and therefore liability and insurance premiums.

1. 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)?

By setting standards which are reviewed regularly to enable them to be updated as technologies innovate, mature and demonstrate reliability the Ministry can provide a framework of trust whilst embracing innovations which benefit consumers.

The ability to verify source of funds, identity and property ownership without having to send copies of documents will vastly improve the privacy and security of identity for home movers.

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

The law is already in place to protect Human Rights and those people with protected characteristics, there is no reason why this should not apply to a digital identity as it would in any other relationship between parties.

Additional benefits of a digital identity will be the ability to reveal only relevant information rather than the whole of the participant’s identifying characteristics.

Those who currently have protected characteristics which make it hard for them to access digital services will quite possibly have a thin digital presence; by creating a digital identity the difficulties which they will experience in providing evidence of their relevant attributes will be lessened. The ability to be able to identify themselves through biometrics could also be advantageous to certain vulnerable customer groups.

As always, there should be the availability of support services to assist those requiring assistance, for whatever reason, in creating and utilising their digital identity.

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

Credit reference agencies appear to be the closest template. They are authorised and regulated by the FCA but they have no requirement to assess the quality of the data being produced.

It would be helpful for a regulatory structure to be provided and supervised to ensure that digital identity providers meet agreed, published and stringent standards of data analysis and protection to deliver a trusted product in the market place.

1. What’s the best model to set the “rules of the road” to ensure creation of this trusted market?

It is likely that there will need to be a statutory framework for the regulation of digital identity and those who certify it. Detailed processes should be devised in a manner which is easily amendable and probably be undertaken by a front line regulator. Light touch audited regulation should be employed to ensure that not only are the standards clearly set out but that the providers can demonstrate appropriate compliance which can be applied in a flexible way so that innovation is facilitated but trust and reliability is not lost.

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

A regulator should be either created or the remit of an existing regulator revised so that the impact of innovation and new technologies and can be assessed and there is a clear remit to provide clear guidance on the acceptability of these developments as they come to the market or risks associated with them.

In the legal industry too much to date is based on outcome based regulation with very little in the way of clear cut examples as to what is acceptable when it comes to digital services.

For example there is no guidance to say that a digital signature is acceptable in the residential conveyancing process and therefore it is very hard for a conveyancer to start to use digital signatures because the other party’s conveyancer rejects it, even though digital signatures have been admissible in court for the best part of two decades.

In all work on regulatory standards the input of users and providers of these services should be sought.

## **Questions on the role of the government**

1. 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?

Yes, obviously with the appropriate anti-fraud protection measures. Currently, whilst it is possible to assess whether a document bears the attributes of an official document there is no service which can confirm that it is in fact a government issued document which belongs to the person purporting to be the owner of the identity.

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

For the purposes of checking that the data provided by the individual is accurate and enabling it to be consumed by digital services which will enable a seamless service which reveals only the information required for the purposes of the enquiry.

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

Any organisation looking to utilise government services for data validation should have achieved a set of required standards evidencing that data protection and processing mechanisms meet stringent government requirements. A complaints process should be embedded to capture evidence of mis-use of data at the earliest opportunity.

Where citizen consent is required they should be given the option to manage the consent so that they have access to give a ‘super-consent’ enabling services which are deemed suitable for the ‘super-consent’ to access their data. They should have access to a dashboard enabling them to toggle an opt in option, potentially via an App for each type of service which might seek to access their digital identity.

  **iii)** What should the cost model be?

Either a subscription model for those entities wishing to access the data for their commercial purposes or a fee per access where the citizen wishes to release access of their identity for a one off purpose.

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

All those with age restrictions imposed by law and protected characteristics where these are relevant in accessing services or might indicate a higher risk of vulnerability which needs to be addressed in the delivery of the service or advice given or the method by which it is delivered.

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

See 15(ii) above. Additionally with legally age restricted products and services it will be incumbent upon the citizen to tell the truth and the use of government data is to verify the information provided so the burden of protection and control by the citizen, where the data is used for the legal purpose, is less.

**iii)** What should the cost model be?

As above.

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

Legislation will be needed to create the framework with which the aims of security, trust and privacy can be met. This is likely to require regulation of the service providers who offer to verify digital identity. Legislation will need to define whether this is done through a revised remit of an existing regulator or by creation of a separate body.

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

Legal Sector Affinity Group Guidance and, in the conveyancing process, the UK Finance and Building Societies Association’s Mortgage Handbooks which currently references a raft of ‘official’ documents which may be relied upon to prove address and identity and the signature of the borrower but contribute to the aversion to accepting digital alternatives.

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

Set clear unequivocal guidance on what purposes the digital identity can be used for and make citizens aware of their ability to set up and utilise a digital identity; and of the protections which ensure that their identity cannot be used for purposes of which they are unaware or to which they have not given their consent.

This could be achieved by sign posting them to do it whenever they interact with government services whether it is in connection with a benefits claim, accessing NHS services, TV licence renewal or taxing their car.

To encourage them to do it, it could be a free service in the first 3 months of them becoming aware of, or eligible for, a digital identity with a regular countdown reminder to encourage uptake ahead of it being charged for.

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

For those wishing to use paper based access to services it will enable local government services to establish their entitlement to those services and prevent fraud.

For those wishing to access services digitally, cost of delivery and administration can be significantly reduced through the use of phone Apps to gain access to services.

Such services can develop over time to enable better use and billing for other local government services and an understanding as to the attributes of those who accesses them, how and why to ensure that benefits of precious resources are maximised.

**Questions on the role of the private sector**

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

The private sector will provide the interface with the means to access the government held digital identity and will be governed by the government created regulator.

By displaying a government approved logo and adhering to the government required standards the public trust and awareness of the initiative will be raised.

Private sector expertise should be welcomed into the consultation processes and ongoing governance and development of standards to ensure that, wherever possible, unintended consequences are avoided and a robust but flexible regulatory environment is created which supports and validates innovation. The participants will have to demonstrate that they can handle information about individuals’ identity with the appropriate protections of their privacy so that data is always used for appropriate purposes and with the knowledge of the individual whose data it is.