INVESTIGATING CHALLENGES IN DIGITAL IDENTITY

Digital Identity Inclusion and Uptake

THE OPEN IDENTITY EXCHANGE |

REPORT WRITTEN BY GARY SIMPSON & EMMA LINDLEY
SOUTH YORKSHIRE CREDIT UNION & INNOVATE IDENTITY

Executive Summary

Digital "***inclusion***" and "***uptake***" are two of the most interesting, and possibly biggest challenges in the adoption of a federated digital identity scheme. Our critical questions in this context are: How do we increase the amount of people that can gain acceptance and access to a digital identity, even in the most difficult to reach demographics in the UK? Secondly, how do we ensure they understand that this identity can be used across more than one service, gaining maximum benefit for all? This small-scale discovery project focuses on the following objectives:

- How could we increase ***inclusion*** through a better understanding of the challenges that hard to reach demographics' might have in the digital identity proofing process?
- How could we increase ***uptake*** and lower the current associated costs within three use cases through demonstration of intent to use additional digital services?

During the ***inclusion*** part of the project a specific group of individuals were chosen on the basis they were assumed to have a low-level of identity footprint. The demographic used was from the Credit Union of which there are just over 1 million members in the UK. These are people who may have no passport, driving licence or other commonly held identity information available, and are therefore potentially difficult to identify. The project was designed to assess the identity challenges with this segment of the population in the context of the Good Practice Guides 45 (GPG45), which are the identity standards, later described in this document.

The second part of the project based on analysing ***uptake***. This was completed to measure increased intent of digital transactions, if citizens that were registered had a single digital identity if he / she would be more likely to access additional public/local authority services digitally. This was compared with the "status quo" where a citizen has numerous passwords and login details to access services. This part of the project focused on areas of current cost and how these might be reduced through the uptake of federated digital identity through the measurement of intent.

The ***inclusion*** part of the project found that in respect to this demographic being able to provide the necessary data / document to allow verification to identity assurance standards within GPG45 Level of Assurance 2, it was found that an average of **24%** of respondents could attain the levels of identity verification and assurance required to transact with most government services.

Secondly it was found that there was between a **10 and 20%** improvement in the ***uptake*** of digital transactions using a digital identity through the measurement of intent, when compared with the current process of multiple user names and passwords to access online services. This correlated with a potential cost reduction of between **£173,419 - £346, 838** across these three transaction types in the South Yorkshire district alone. This represents a huge potential saving for this Local Authority.

Table of Contents

About Projects

In order to hasten adoption of the IDAP Framework there is a practical and strategic opportunity to leverage OIX domain expertise. OIX facilitates and coordinate the rapid formation and deployment of *White Papers*, *Discovery* and *Alpha Projects* in an agile manner.

These are defined as small scale, low risk assessments, analyses or tests of interoperable components that address the key challenges of the IDAP goal to create convenient, secure, and privacy-enhancing digital transactions.

This small-scale project indicates that the demographic within the test do have challenges with the creation of a digital identity. However if they had a digital identity they would be inclined to increase the amount of services they accessed which could result in huge cost savings. Full details of the project method, outcomes and recommendations can be found in this document.

1. Background

Within the UK there is no single authoritative source or credential, which can be used for asserting identity securely in an online transaction. 36 million adults (75% of the adult population) in Great Britain are now online everyday, and 72% of these adults buy goods or services online. These statistics, combined with the increased sensitivity of online transactions e.g. banking, government creates a challenge for organisation's that need to verify and authenticate the identity of each one of its citizens or customers.

In particular as we see government services move online we need to consider the security required for accessing online healthcare records, employment benefits and taxation, and recognise that these types of transaction require an increased level of security when it comes to the assertion of identity.

In order to address these issues the UK government created the Identity Assurance Programme (IDAP), the purpose of which was to create a means by which individual citizens could create, manage and make use of a single digital identity, which could be applied across multiple services and sectors.

Within the first procurement five companies have signed contracts to provide such services. Working under a detailed identity assurance framework, the IdPs can access private sector credit record information, and certain government data, so as to be able to ascertain – with a high level of assurance – that the person creating and using a digital identity is who they claim to be.

Levels of Assurance

Different types of service require different levels of assurance that the digital identity being invoked is current, correct, and being used by the individual to which it relates / belongs.

- ***Level 1*** At Level 1 there is no requirement for the identity of the applicant to be proven. The applicant has provided an identifier that can be used to confirm an individual as the applicant. The identifier has been checked to ensure that it is in the possession and / or control of the applicant.

- ***Level 2*** At Level 2 identity is a claimed identity with evidence that supports the real world existence and activity of that identity. The steps taken to determine that the identity relates to a real person and that the applicant is the owner of that identity and it gives sufficient confidence for it to be offered in support of civil proceedings

- ***Level 3*** At Level 3 identity is a claimed identity with evidence that supports the real world existence and activity of that identity and physically identifies the person to whom the identity belongs. The steps taken determine that the identity relates to a real person and that the applicant is the owner of that identity to give it sufficient confidence for it to be offered in criminal proceedings.

For further information on levels of assurance, as defined by the CESG - the National Technical Authority for Information Assurance, see

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/270964/GPG_43_RSDOPS_issue_1.1_Dec-2012.pdf

2. What is Digital Identity?

A digital identity is a way of a person asserting that "they are who they say they are" online as well as offline. It is created using a set of verified attributes or data protected by a set of secure credentials. The security is designed so that the digital identity can only be asserted, accessed and used by the person to which that identity belongs. This process is referred to as Identity Assurance.

Within the context of the Identity Assurance Scheme in the UK there have been standards created by which Identity Assurance operates under. These standards are called the Good Practice Guides (GPG's). Within GPG number 45, the standard that is associated with the identity proofing and verification, the information required to support the validation of the attributes is sorted into three categories, Citizen, Money and Living https://gds.blog.gov.uk/2012/05/14/good-practice-guides-enabling-trusted-transactions/

Within these categories the citizen is also required to provide not only evidence of their current identity but also historical identity information called "activity history", for example financial history with their bank. The GPG's define how these attributes from the relevant categories (C,M,L) can be asserted and validated for the citizen or individual to have their identity assured to enable the transaction they wish to do. For example if the user wanted to complete a transaction to access their driving license records there would be a level of identity assurance required to be attained to make that type of transaction. In the context of identity assurance these are called Level's of Assurance or LoA's.

Identity Footprints

- ***Thick file*** individuals have a high level of digital records with their details. The majority of UK citizens have **'thick' files**, which can be used to verify their identity e.g. financial records, council tax or utility bills in their name.

- ***Thin file*** individuals do not have some of the traditional forms of identity credentials at their disposal. Examples include young people, ex-military and recent immigrants. These groups may have difficulty verifying their identity.

Levels of Assurance

Levels of Assurance are put into 4 categories 1 – 4. LoA could feasibly allow the user to complete different types of transaction dependent on the security requirement or perceived risk with that type of transaction. The user needs to provide more information to prove their identity the higher the LoA.

3. Digital Identity Challenges

Within this project we investigated two digital identity challenges, ***inclusion*** and ***uptake.***

Inclusion

With so many more of the UK population now interacting and transacting online, it means that there is additional requirements to create online "trust" to reduce the risk of online fraud. The creation of digital identities through a framework of standards and governance is a method to create this trust. When organisations can trust more people online through the use of digital identities it will mean more services and transactions can move online, resulting in huge cost savings.

However it is possible that not all citizens of the UK will have enough verifiable identity attributes to gain the appropriate level of assurance to allow them to create a digital identity and complete the transactions they wish easily. It is possible that all UK citizens do not hold some of the verifiable identity attributes accepted to create a digital identity to the higher levels of identity assurance.

For example in the UK around 75% of the population have a passport and 76% have a driving licence. Many people are not registered to vote and therefore these details cannot be verified. This could create a challenge for identity assurance by making the passage to obtaining a digital identity for some citizens difficult.

Identity Footprints

- *Thick file* individuals have a high level of digital records with their details. The majority of UK citizens have **'thick' files**, which can be used to verify their identity e.g. financial records, council tax or utility bills in their name.
- *Thin file* individuals do not have some of the traditional forms of identity credentials at their disposal. Examples include young people, ex-military and recent immigrants. These groups may have difficulty verifying their identity.

Uptake

Another challenge of identity assurance is to enable the potential financial benefits that a ubiquitous federated digital identity could bring.

At present citizens have different user names and passwords for most transactions online e.g. a doctor's online appointment user name and password will be different to the user name a password requirement for accessing a financial services product. These requirements to use multiple user names and passwords create headaches for both the citizen and the organisation.

As a consequence of these difficulties interacting there are use cases, which may be more difficult, online. Cancelling a doctor's appointment, accessing financial information or a tenant reporting a fault with their property. There is a cost associated with these use cases that could be reduced if it were proven that a single digital identity made it easier to transact across services without the need for multiple user names and passwords.

Commercial Considerations - Uptake

There were three use cases for the uptake part of the project. These were aligned with commercial costs taken from each of these organisations within the target area of South Yorkshire. (Berneslai Homes – Barnsley Council ALMO), a credit union (South Yorkshire Credit Union) loan application, and a doctors appointment (making or cancelling). It was considered that all three of these services would be greatly enhanced by providing a mechanism to help the citizen manage these events in a simple way. In the example of doctor's surgeries and housing association's missed appointments is a significant cost. The hypothesis is that if patients / tenants had a digital identity and it was made easier to make and cancel appointments online then there would be less missed appointments.

For the Credit Union there is a cost of verifying the identity of each applicant before providing a Credit Union account. If the applicant already had a digital identity they may not be required to do this verification themselves, saving £14 per applicant.

The project's trial was designed to measure the percentage increase in the propensity to use such services using a single digital identity versus the status today where people have to use multiple user names and passwords. This in itself would provide direct cost savings but also opportunities for all parties to actually improve, grow and sustain services.

Examples of the commercial considerations and the potential savings are shown below based on the services selected by this project and included in the *uptake* element.

Berneslai Homes

No. of Tenants Appointments/Year	No. of Missed Appointments/Year	Average Cost of a Missed and Rearranged Appointment (lowest costs estimated)	Total Est. Saving/Year
18,564	734	£25	£18,350

South Yorkshire Credit Union

No. of Loans (12 months)	Est. Saving per Loan/using POID	Total Est. Saving/Year
14912	£14	£208,768

Barnsley Health

No. of Appt/mnth/surgery	No. of DNA/mnth/surgery	Average Cost/Appt	Cost of DNA/mnth/surgery	Cost of DNA/year/surgery	No. of Barnsley Practices	Total Cost to "Barnsley"
1539	128	£20.16	£2580.48/mnth	£30,965.76	38	£1,176,698.80

Fig 2.

Project Hypothesis

Below are the statements tested during the discovery project:

1. That this demographic from South Yorkshire would not have sufficient identity attributes, which could be validated to gain LoA2.
2. That having a digital identity would mean more people would transact multiple times than when using three sets of user name and passwords.

Digital Inclusion

- *Expected "thin file"*
- *Credit Union customers*
- *Two groups of 22 people*

Project Participants - Credit Union

Credit Union customers were asked to participate in the trial. This is because Credit Unions typically deal with citizens who have had difficulty gaining access to the usual method of banking or financial services products. For some in this demographic their lack of identity evidence leads to difficulty with the financial services industry process and regulation relating to identity verification, known as Know Your Customer (KYC). It was assumed this demographic will have difficulty presenting enough identity information in the context of this project.

5. Project Method

Digital Inclusion

A pre-agreed questionnaire was compiled across all three participating IdPs for a survey of thirty-two participants, all of whom were members of the South Yorkshire Credit Union. The survey was completed with full consent and details of the individuals were anonymised. The participants were asked to provide details within the survey, which allowed the assessment of identity evidence they had in relation to GPG45 and LoA2. The results were collated and assessed.

Digital Uptake

This part of the research used mixed methods to ascertain whether a single sign-in process would increase the propensity for a low identity footprint and "thin file" demographic to access online public services. Two groups of 22 people were each given an online task to complete. One using single sign-in and the other one using an existing multiple sign-in process. This was introduced to them during a number of face-to-face workshops with a user researcher. The project technology partner, Looking Local, mapped this task onto an existing application.

Use Cases - Intent

- *Tenant Repairs*
- *GP Appointments*
- *Credit Union Account*

Method

- *PC*
- *Tablet*
- *Smartphone*

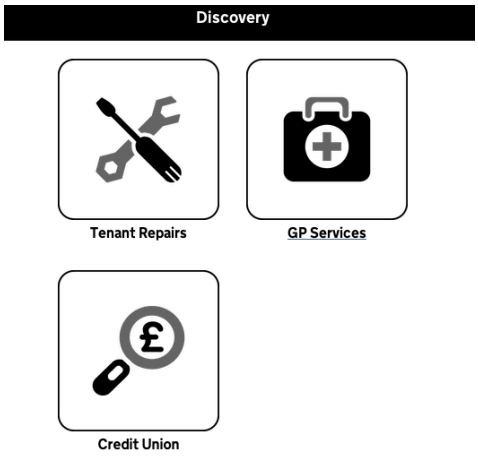

Fig 3.

The online task consisted of giving each respondent an online task to do in their own time using whatever technology they would ordinarily use (PC, tablet, smart phone). The task was for them to attempt to make two tenants repair applications, one GP appointment and one check of their Credit Union account.

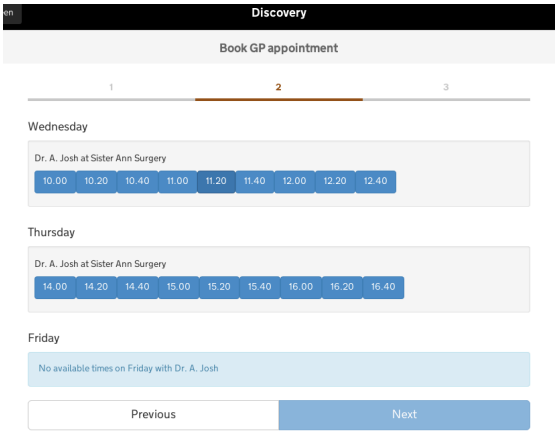

Fig 4.

The results were assessed through analytics of how long the process took to complete and also places within the process that respondents stopped completing the process (through confusion, complexity or other). The user researcher then contacted a selection of the respondents to gain further feedback.

User Comments

Below are the comments from the respondents in relation to the increased ease of the single sign up process:

User 1

"It was really simple, I wish making a GP appointment was that simple [...] great being able to go from one service to another, made it really quick [...] much easier than using lots of login. I have loads of trouble remembering them all even though they're quite similar - I just change one or two numbers for each - but this would be much better".

User 2

"One password might make it simpler for me but not a lot simpler as I only have one password [for my logins] anyway."

User 3

"Though I would want to know that the security was OK, being able to see my credit union account easily worried me a bit". Wanted reassurance on when the PIN would be used - was it a one off or would it be used for each session.

6. Findings

Digital Uptake

With regard to ***uptake*** the findings point to an increase of **10 -20%** in the propensity of people from this demographic to complete multiple tasks via single sign-in.

This increase of digital uptake if referenced against the suggested areas of cost could mean between a **£173,419 - £346, 838** cost saving across these three transaction types in the South Yorkshire district. This cost saving is due to the anticipated reduction in missed appointments across doctors surgeries and tenants repairs, and also to the reduction in cost of identity verification for the Credit Union.

Users also spent less time on the pages within the forms. This was attributed to the fact they do not have to login to access the different areas, and can move around the site more easily.

Fig 5.

The design of the test system resulted in the time taken to login being slightly higher on the single sign-in process, due to an additional layer of two-factor authentication (in the form of a code being sent to the mobile phone). Without this additional layer of security the direct comparative log in times can be seen in Fig 5.

Respondents Comments

Below are the comments from the respondents in relation to the problems they encounter when trying to make a doctors appointment online:

"I have tried and it's useless to be fair"

"Yeah it's not very good. I thought I'd have a go because its absolutely shocking trying to get an appointment in me doctors"

"And so I thought' oh I'll have a go and see if I can work this online business out, I went to the doctors and they gave me two pieces of paper with loads of different pin numbers…"

"If I could book an appointment with the doctor online I'd do that every time…I spend ages on the phone, trying to get through. It can take forever then you find out they don't have any time to see you"

Other interesting findings included:

Online identity is badly managed and a security concern.

19 of the **22** people spoken to in the groups used one password (and sometimes a simple variation of that) for all their online identities. They seemed aware of the inherent security risks associated with this behaviour but couldn't see a way to easily manage their identity any other way. Banking service and other financial services such as PayPal were more frequently mentioned as "best of breed" in managing identity. It is clear that "identity management" means very different things to different people.

Habit and frequency affect identity in practice. Only a few services were used very frequently. Most respondents used Facebook, although this was more used by the female rather than the male respondents. Some of the male respondents viewed it as a place for gossip and "tittle tattle". Other sites that were popular included eBay, retail sites such as Play.com, ASOS, Argos, Tesco and Amazon. A minority citing betting services, Skype and Internet utilities as sites they used frequently.

Most stated that public services online do not have the same frequency of use and as such ways to access them online fail to become a habit meaning that any login details, processes or passwords were generally forgotten.

Sharing is commonplace. Many in this demographic share identity information. Partners, friends and family managed Credit Union (CU) identities, shared Facebook and Twitter profiles as well as other account details. It can be a form of social capital (when it's on agreed terms). This is of huge importance to the identity community, if details of these accounts are shared how would this be identified over fraudulent account takeover.

Mobile and email are a weak anchor to identity. Email and mobile phone numbers are not a reliable validation or recovery mechanism alone. Email account and sims / mobile numbers (and phones) were frequently changed, forgotten, shared, lost or traded.

“uptake”

noun
“the action of taking up or making use of something that is available.

Uptake Findings

Online identity is badly managed and a security concern

Habit and frequency affect identity in practice

Mobile is a weak anchor to identity

Sharing is commonplace

Mobile passcodes wanted as universal logins

This was demonstrated when the user researcher tried to contact many of the respondents for further feedback only to find their mobile number had indeed changed.

Identity is about ‘now’. The frame of reference for identity seems fluid amongst this audience. Their frame of reference tends to the ‘now’ as many don’t have an identity that is meaningful (for example, few have a credit rating) to value in the longer term, so starting a new identity, a new account, often isn’t a big deal. Creation of multiple accounts affects many organisations, managing these multiple accounts creates an expensive overhead. Additionally organisations don’t know (without analysis) how many customers they actually have.

Mobile passcodes act as universal logins. Uses of native apps on mobile seem to have different login behaviour. The phone passcode itself is often seen as a login, with most native apps set to be logged-in to automatically. Peoples’ identity is bound up within the phone and the native apps are an extension of that. The same is not true of services access through a desktop browser. What is clear is the perception of security is not the same as what is actually deemed as secure.

Inclusion

With regard to ***inclusion*** there were many valuable findings in addition to the core identity information, which could shape the thinking of methods of identity verification and on-going communication with this, demographic in the future.

Smartphone usage was prevalent amongst the participants with **87%** responding that they accessed the Internet using one. For **23%** of participants a smartphone was their only means (from a choice including tablet, desktop and laptops) of accessing the Internet.

All participants stated that they owned a mobile phone. Just over half **(53%)** of these were on a post pay contract with the remainder

Inclusion Findings

87% of respondents accessed the internet using a smartphone

47% has a pre-pay mobile phone contract

94% said they had a Facebook account

Twitter was the second most used social network

(47%) on prepayment - pay as you go. Of the mobile phones, only one participant did not have smartphone.

Android was the most common operating system **(52%)**, Apple iOS the next **(42%)** with **3%** each for Windows and Blackberry.

Rather surprisingly all participants bar one 17 year old were present on the credit referencing data, which was validated against for identity purposes. However they did not have the history contained within the credit file due to the fact they were now using the Credit Union and this data is not shared with the Credit Referencing Agencies.

In relation to social media **94%** of individuals said they had a Facebook account with the next largest group on Twitter followed by Google Plus.

The three IdPs noted against their current citizen on-boarding processes and current identity requirements to attain Level of Assurance 2, this included whether the participants owned passports, driving licences and had bank accounts, along with the required identity history. The average rate of successful citizen on-boarding to Level of Assurance 2 was 24%.

This is considered lower than the percentage for other demographics of UK citizens. Activity history evidence seemed to be one of the critical factors missing which reduced the number of individuals gaining a Level of Assurance 2.

Conclusion and Next Steps

This ground-breaking insight into the selected citizen demographic has allowed testing of the hypothesis for both uptake and inclusion with demonstrable monetary cost savings. It demonstrates that through collaboration of the industry we can make incredibly insightful conclusions about direction for further investigation. This project holds the key to identifying and unlocking the issues about one of the areas of digital inclusion for this demographic.

There is a clear indication that uptake of digital transactions could be improved through the use of a digital identity in comparison to the status quo of multiple user names and passwords. The additional ease by which people could interact with both public and private sector services mean hard cost savings could be made. In the example of doctor's surgery appointments the increase ease by which a confirmed appointment could be cancelled could lead to a subsequent cost reduction. The lack of cancellation of a doctor's appointment is not a malicious act by the patient, simply a task which takes effort through a method (the telephone) which often means delays. This could be improved by a seamless online experience.

Further insight into the types of additional security layers would be an interesting area here for future research. What kinds of security measures create confusion and perhaps citizens dropping from the process? Are security measures contextual to the transaction and how would we measure this?

What is clear is that user research is critical in the investigation to the uptake of identity. Conclusions about what will or will not work for the user cannot be made in isolation of the user, if they are, there is a significant risk that users simply will not engage. The balance of security and citizen / customer experience must be considered carefully if the aim is to engage all potential users. Rather than putting methods of security in front of the user that they do not understand or want to use, thought should be given to understanding what users ***consider secure*** and ***want to use***, then looking at ways to make them more secure if required.

People seemed very appreciative of services that helped them manage and recover their online identity, services such as PayPal, Banks and Google (through 2 step authentication), and Facebook were mentioned in this regard. Framing this federated identity to work as a way to both save time but also to be secure.

This demographic are closely networked and have a strong sense of community they will often ask one another for help or advice. Word will tend to spread about bad or good experiences with

products or organisations. Efficiency gains are not universally appealing to this demographic, but financial incentives are. Money off vouchers, especially with mobile phone top-ups or contracts or grocery shopping would likely lead to significant improvements in online conversion and more frequent touch points to manage online identity.

Customers with a lack of available identity evidence footprint and activity history may be excluded from being able to verify their identity until such time as richer and more robust data is available for this demographic. Further insight into what the alternative sources of data that could be used for identity evidence with this demographic would be useful. In addition an understanding of whether those data sources are available for use immediately or if there are technical, privacy or access restrictions to that data.

One consideration could be to investigate the way in which positive information about individuals could be shared with Credit Referencing Agencies to prevent digital history "drop off" when they move from traditional banking networks to Credit Union networks.

A second consideration could be to look at the use of offline documents such as utility bills, birth certificates and others to see if there is a way these documents could be digitised in a secure way.

A third consideration could be given to the work done in the "Use of Mobile in Identity" project. This project looks at how mobile can be used as an authentication method and mobile data could be used for identity proofing evidence. Given the wide spread use of mobile by the participants within this project, further investigation would seem sensible. It has to be noted that there is some conflict in the findings about the use of mobile within identity due to the propensity to change numbers and share mobile phones.

It is also noteworthy that this particular demographic taken from the Credit Unions may not be the only demographic that have a low level of identity footprint, students, the elderly, new entrants to the country or those people that only operate in cash may also be affected in the same way.

This is not an exhaustive list but seeks to focus direction in areas which positive changes could be made. The use of citizen data is an area where Government and Identity Providers can work together to deliver innovative solutions backed by data currently in existence. A collaborative effort by government, identity providers and data providers is needed to support the ability of 100% inclusion for all UK demographics.

-End-