OIX℠ OPEN IDENTITY EXCHANGE

DIGITAL SOURCES OF TRUST

White Paper

Edited by Livia Ralph

May 2015

Contributors

Adobe

SOUTH YORKSHIRE CREDIT UNION LTD
SAVINGS & LOANS CO-OPERATIVE

Cabinet Office
Government Digital Service

OIX OPEN IDENTITY EXCHANGE

mydex

Skills Funding
Agency

POST OFFICE

Experian

Rattle

Validoc
Documents validated at source

OIX UK is the UK arm of a global organisation and works closely with the Cabinet Office on the Identity Assurance Programme. Its goal is to enable the expansion of online identity services and adoption of new online identity products. It works as a broker between industries, designing, testing and developing pilot projects to test real use cases.

Executive Summary

Digital channels are increasingly important for transactions of all types. However, verifying a person's personal details in a digital transaction remains a time consuming and complex process. For many people the difficulty of proving identity stops them from completing transactions or registering for new services.

The 'Digital Sources of Trust' (DSOT) discovery projects have investigated the challenges of identity verification for users that do not possess traditional identity credentials such as a passport or driving licence. The majority of the users interviewed in these projects expressed a need for a process where verification of their identity would be made easier. At present they face numerous barriers (and additional, often crippling costs) or lengthy processes to verify their identity, even for simple things such as application for a course. Most of these people have evidence of long customer histories with public and private sector service providers but the evidence is largely paper based and therefore of no use in a digital transaction.

A new market of services is developing that makes it easier for people to verify their identity when conducting digital transactions. However, these services are dependent on access to data from authoritative sources by mechanisms that are trustworthy, compliant with data protection laws and commercially viable.

The Digital Sources of Trust discovery projects have considered three such mechanisms from the perspective of the individual user. By placing the user at the centre of the transaction and designing the process with the user's privacy in mind it is possible to design solutions that work to the benefit of all parties.

The project's main focus has been on mechanisms that allow individuals to use their data as evidence in a trustworthy way. There are many data sources, both in the public and private sector, that could be used as evidence of identity. However, the project has sought to identify how the data sources can be used to provide control to the user, align with privacy principles and legal requirements and be commercially viable to all the organisations in the value chain. Three mechanisms have been considered within the project; a 'digital notary', a direct attribute provision service and a Personal Data Store (PDS).

The OIX UK project was initiated in support of the UK Cabinet Office's GOV.UK Verify service. The Government Digital Service (GDS) programme aims to expand the range of evidence people can use to verify their identity. This document summarises the findings of the work conducted so far. It is anticipated that further work will be conducted through OIX UK over the summer of 2015.

1. Background, Objectives and Hypothesis

Table of Contents

Background

Individuals, when proving their identity, use various data they possess so organisations they interact with can verify that these individuals are who they say they are. The widely used and accepted identity documents such as passport, driving licence or birth certificate, however, are not possessed by everyone. Therefore many people use other forms of data available to them to prove their identity.

For example, many people use utility bills, bank statements, council tax bills and others. Often these documents are issued digitally and the customer needs to print them out to use in other context (and prove their identity). Yet, many organisations do not accept self printed copies of those items as evidence. Where available, the process of verifying these documents is costly and time consuming for both the organisation verifying the identity and the Issuing Authority (IA), the organisation that issued that particular document.

At the same time quite a large part of UK population falls into financially, digitally and/or socially excluded groups[1]. This implies that there is a 'digital identity gap'[2] which would include all three of these overlapping, excluded groups of a minimum of 19% of the population.

The Identity Assurance Programme (IDAP)[3] which is working on the development of GOV.UK Verify, an online identity assurance service for government services, has developed Good Practise Guides (GPGs) - a set of guidelines for Identity Providers (IdPs) who are responsible for verification of identities of those that use online government services. According to Good Practice Guide 45 (GPG 45)[4], Identity Providers need to confirm evidence to be valid and/or genuine in order to meet the requirements for achieving Level of Assurance (LoA) 2, the standard Identity Providers are contracted to meet under the current Government Digital Service (GDS) procurement.

[1] The stats provided in BBC report 2014 Digital Skills note 19% of UK population do not have basic online skills, p.2, http://bbc.in/U0BEY7

[2] http://linkd.in/1bXnGj6

[3] Identity Assurance Programme (IDAP) is part of the Government Digital Service in Cabinet Office, that is responsible for the GOV.UK Verify service and other related products and services

[4] http://bit.ly/1ptVm91

The Digital Sources of Trust project investigated how users can present evidence of identity through mechanisms that meet the UK standards for identity verification. The project was split into two parts: Project 1 looked at purely online user journeys and concentrated on a direct attribute provision service and a Personal Data Store (PDS); while Project 2 looked at paper evidence and the use of QR codes to validate this evidence.

Customer insight research was conducted in which users simulated verifying their identities through the different methods. The users were selected to represent the demographic described above. The researcher elicited the user's attitudes to the individual methods throughout the simulated customer journey. Further detail of the testing methodology and results can be found in the appendices to this summary document.

DSOT 1 participants included Skills Funding Agency (SFA), Adobe, and GDS, while DSOT 2 included South Yorkshire Credit Union (SYCU), Validoc, Doncaster College, and GDS.

Objectives:

The objectives of the project were to discover:

- The user experience under which users would be inclined to present digital evidence of identity from trustworthy sources to a certified Identity Provider (IdP) as part of identity registration.
- The user experience under which users would be inclined to present paper evidence of identity from trustworthy sources to a relying party (in this instance South Yorkshire Credit Union (SYCU)) as part of their Know Your Customer (KYC) checks when registering for an account.
- The business process for services by which data or evidence can be determined as 'valid' or 'genuine' or both by Identity Providers in order to meet the requirements set out in GPG 45.
- The open specifications that enable Issuing Authorities to make evidence available to users in ways that score 2 or 3 for elements A and B of the Identity Proofing and Verification process as defined in GPG 45.
- The privacy and data protection principles that need to apply to the design of the service and its interfaces.
- processes that would allow Issuing Authorities and users to go paperless when verifying their identity or would allow them to apply measures that facilitate current paper based processes.

Hypothesis:

The projects looked at how people who do not have 'traditional' evidence of identity could use data from other sources to verify their identity to a third party.

They tested the following hypothesis: 'Individuals would be inclined to use alternative methods of verifying their identity both in an online and offline environment, respectively, if they were given the option to do so.'

Researcher: *"We are trying to understand how you prove who you are."*

User:*"It's really hard. It's a pain in the backside because you take your whole life up in one folder to them. Things like when I've done a college course you'd think I was trying to apply for a mortgage, it was like "have you got any ID" and I said, no not really and they said "passport"? and I said no it ran out years ago and I haven't needed to go abroad [...] "driving licence" and I was like "I don't drive" and they said so what have you got and I said "tenancy agreement, council tax letters and they said "well we need photographic proof of who you are [...]" so I've had to take a massive folder of stuff and it's still not good enough. Finally I had an old post office staff card with my photo on and they took that" (F, 34, London)*

2. Focus of user testing

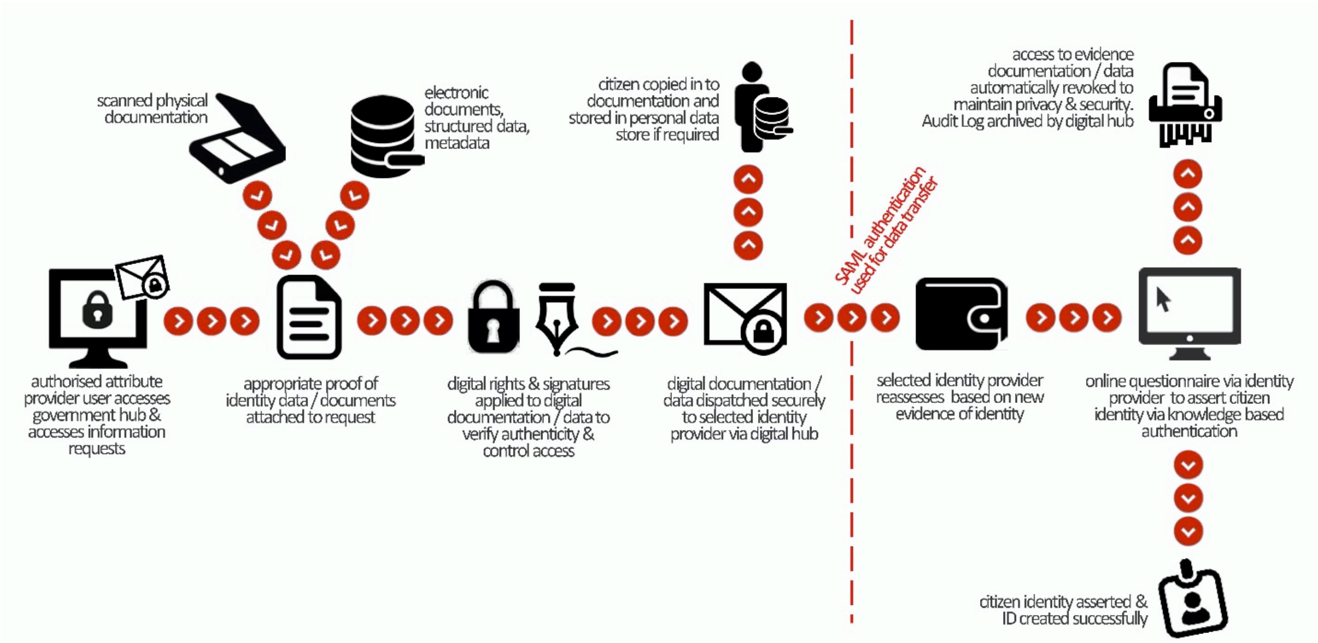
Both projects focused on a particular demographic, the 'thin file' group - individuals who do not possess some of the traditional forms of identity credentials such as passport and driving licence: documents usually required by organisations that need to verify individuals to a certain level of assurance in order to provide a service (such as opening a bank account). The 'thin file' descriptor can also be applied to many people who do not have accurate records in data sets commonly used for identity verification. However, typically it applies to young people, ex-military, recent immigrants, and those who are financially, socially, or digitally excluded.

People within this particular demographic often find it difficult to verify their identity. This in turn has a knock on effect on what services they can access both in face-to-face interactions and online. They struggle with simple things such as applying for a course (see quote). The process is too burdensome and complex. The project explored methods that would reduce the burden of verifying individuals' identities and would also allow them to access new services.

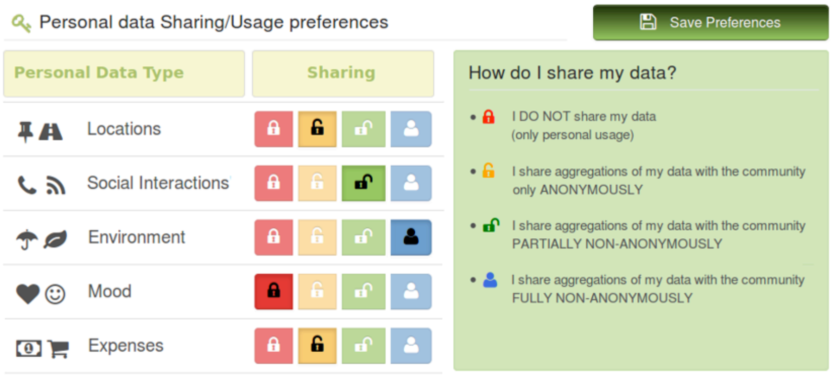
3. Methods explored

The two projects looked at three different methods of how attributes people possess could be used to verify their identities.

Project 1 looked at how, by using Adobe PDFs with the application of Digital Rights Management (DRM), electronic documents could be consumed by the Identity Providers directly from Issuing Authorities, with the user's consent, and feed into the verification process. The user research considered a user journey where the metadata from an SFA Personal Learner's Record could be used to develop Knowledge Based Verification (KBV) questions users would have to answer while creating an account with an Identity Provider.


scanned physical documentation
electronic documents, structured data, metadata
citizen copied in to documentation and stored in personal data store if required
access to evidence documentation / data automatically revoked to maintain privacy & security. Audit Log archived by digital hub
SAML authentication used for data transfer
authorised attribute provider user accesses government hub & accesses information requests
appropriate proof of identity data / documents attached to request
digital rights & signatures applied to digital documentation / data to verify authenticity & control access
digital documentation / data dispatched securely to selected identity provider via digital hub
selected identity provider reassesses based on new evidence of identity
online questionnaire via identity provider to assert citizen identity via knowledge based authentication
citizen identity asserted & ID created successfully

The second method tested looked at PDFs and metadata from these documents being shared by individuals through their Personal Data Store (PDS). This approach would allow users to share evidence they chose from the PDS during creation of an account with an Identity Provider.



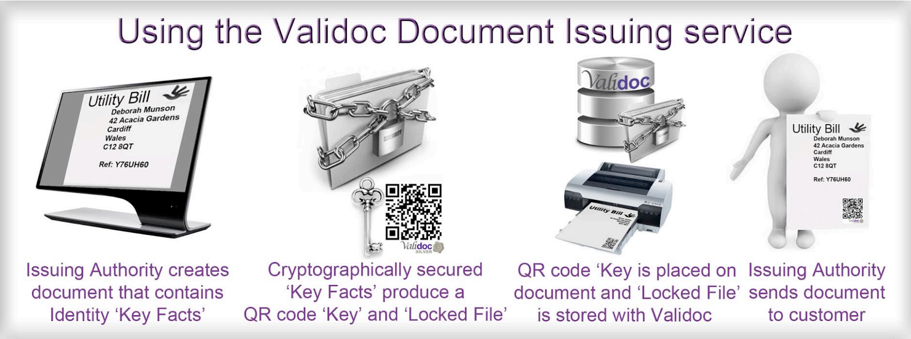
Personal data Sharing/Usage preferences

Personal Data Type	Sharing
Locations	🔒 [✓ 🔓] 🔓 👤
Social Interactions	🔒 🔓 [✓ 🔓] 👤
Environment	🔒 🔓 🔓 [✓ 👤]
Mood	[✓ 🔒] 🔓 🔓 👤
Expenses	🔒 [✓ 🔓] 🔓 👤

How do I share my data?

- 🔒 I DO NOT share my data (only personal usage)
- 🔓 I share aggregations of my data with the community only ANONYMOUSLY
- 🔓 I share aggregations of my data with the community PARTIALLY NON-ANONYMOUSLY
- 👤 I share aggregations of my data with the community FULLY NON-ANONYMOUSLY

Project 2 looked at existing paper documents individuals possess and how these could be validated in alignment with government standards when checked. The project looked at the use of QR codes on the enrolment letters received from Doncaster College and their verification by South Yorkshire Credit Union while opening an account. South Yorkshire Credit Union, as part of the registration process, checks a number of documents individuals use as proof of their identity. In this instance, the QR code on the document when combined with data on the Authoritative Source server verifies the authorship and contents of the documents. This was done through the use of a simple application installed on a smartphone/tablet and allowed for it to be done in a way that is compatible with the government standards. The project also considered a user journey where existing South Yorkshire Credit Union members received paying-in books with QR codes on them and used them at South Yorkshire Credit Union to check their balance.



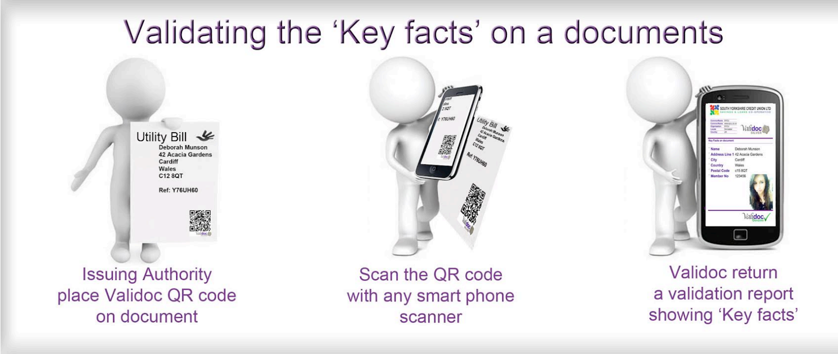
Using the Validoc Document Issuing service

Issuing Authority creates document that contains Identity 'Key Facts'

Cryptographically secured 'Key Facts' produce a QR code 'Key' and 'Locked File'

QR code 'Key is placed on document and 'Locked File' is stored with Validoc

Issuing Authority sends document to customer

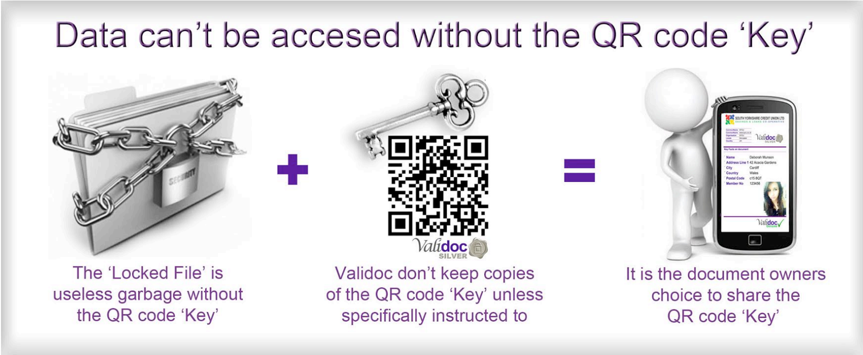


Validating the 'Key facts' on a documents

Issuing Authority place Validoc QR code on document

Scan the QR code with any smart phone scanner

Validoc return a validation report showing 'Key facts'



Data can't be accesed without the QR code 'Key'

The 'Locked File' is useless garbage without the QR code 'Key'

Validoc don't keep copies of the QR code 'Key' unless specifically instructed to

It is the document owners choice to share the QR code 'Key'

The detailed user journeys can be found in Appendix A along with the link to full project reports.

4. Findings from explored User journeys

There were some commonalities across all the user journeys explored. The majority of the users expressed a need for a process where verification of their identity would be made easier. At present they face numerous barriers (and additional, often crippling costs) or lengthy processes to verify their identity, even for simple things such as application for a course. They do not possess traditional identity credentials such as a passport or driving licence. Using credentials that they already have would therefore ease their lives.

View of using Verify

"That would be a good service. I reckon a load of people would start using that because some people they might have to carry one thing to bank with them, other might need to carry passport, birth certificate, letters and end up carrying a big bag full of paperwork. With this, if you (Verify) was [sic] registered with banks and that as well you'd be able to go online apply for a bank account and get a card in the post because they've verified who it is already." (M, 28, London)

Conversion: The possibility of being able to verify a user's identity through knowledge-based verification or sharing data via a Personal Data Store, was perceived very positively, as at present the thin file cohort find it difficult. Only three out of 20 would not have completed the process online and would have rather used an offline channel. This was due to lack of confidence in their ability to complete the process correctly (two of the three) and lack of trust in online verification (one of the three).

Understanding: Most participants did not understand what was being shared, with whom and how it was being shared. The main concern of users was sharing information they saw as very personal with a third party.

Privacy: Respondents felt that questions such as grades from various courses were too *"in your business"*. They were very reluctant to share financial information - both account based information and also transaction or activity-based information. The heightened wariness around financial data is possibly due to this information being used to control their access to services in the past. Moreover, financial activity lays bare decisions they've made (for example prioritising to spend money on clothes rather than rent), and their financial status. User journeys - both with knowledge-based verification or with the use of PDS - would in the future require clearer communication with the user about what is being shared and in what format.

Findings from DSOT 2

Conversion: Most participants (over 80%) rated the experience as better than either a typical bank registration or a South Yorkshire Credit Union transaction. Whilst many did not possess an understanding of what QR codes are (and this was not explored in the project), users understood the role they played in the process of registering and transacting with the South Yorkshire Credit Union and they appreciated that it made the process of transacting quicker and simpler.

Processing: South Yorkshire Credit Union staff found the process of using the QR codes simple, the learning required almost negligible (they were able to use software installed on most smartphones).

Trust and Risk: The main benefits to the staff in using the QR codes to check validity of the document and the data in the document, was that it significantly reduced the risk of forgeries being passed through as evidence.

"Much easier than registering at a bank. Or trying to" (F student, 18)

"It's very simple to use" (Kat, SYCU)

"We get people forging documents [...] this would help us to stop that." (Kat, SYCU)

Additional findings

The research also included a number of group sessions and interviews with the thin file cohort that looked at identity and associated issues. The main points coming out of these sessions were:

Cost: the cost of identity documents such as passport or driving licence proves too much and as such discourages this particular group from getting this type of identity document.
Cascade effect: when people lack core identity documents such as a passport, driving licence or birth certificate trying to then obtain any of them becomes more difficult and challenging.
Concept of identity: understanding of identity varied across thin file cohort. Young people were more familiar with the concept as they use social media on a daily basis.
Value is driven by access: the value of documents was based on what they could provide access to and photo ID was considered to be most valuable (a Photo ID bus pass was more helpful to people than a birth certificate on a day-to-day basis).

5. Conclusion and recommendations

User testing explored user journeys that would allow citizens to use attributes they currently possess, such as enrolment letters, their personal learning records and others, to help prove they are who they say they are. The user research undertaken highlighted the need for such services as numerous users expressed the need/desire and excitement for something like this. The discovery project has proven that the hypothesis it tested, 'Individuals would be inclined to use alternative methods of verifying their identity both in an online and offline environment, respectively, if they were given the option to do so.' is valid and is worth exploring further.

Overall, users welcomed these methods as they saw them as key to solving issues associated with verifying their identities. They noted numerous benefits such as time saving, convenience, access to additional/new services and others. These methods would also ease users' registration for a digital identity with the Identity Providers to the required Level of Assurance and allow access to public sector services available through GOV.UK Verify. The detailed learnings, benefits and barriers of the methods explored, to all parties involved, can be found in Appendix B.

Following the successful discovery project the recommendation is to move into an alpha project. The alpha project should explore full end-to-end user journeys (from using an enrolment letter to open a South Yorkshire

Credit Union account to creating a digital identity with GOV.UK Verify), using metadata provided in secure PDFs and QR codes on documents. Both methods are complementary and should be explored in joint alpha.

The alpha project should also consider the high level design needed for these methods to integrate with GOV.UK Verify and its Identity Providers, and consider the commercial aspects of the design. It needs to focus on user-centric propositions. It is also recommended that the alpha project considers 'thin file' in the wider sense and tests the user journeys across wide spread of thin file demographics in order to get a better understanding of how scalable such methods are.

Appendix A

Both project reports that focus on the user research aspect of the two projects can be found here:

Digital Sources of Trust 1 Discovery Project Report

Digital Sources of Trust 2 Discovery Project Report

User journeys explored:

DSOT 1 User journeys:

1. User journey 1:
    a. User is applying for a provisional driving licence online.
    b. User is redirected from the service provider to GOV.UK Verify to register with one of the Identity Providers (IdP).
    c. User chooses one of the Identity Providers to register with.
    d. While registering with an Identity Provider User chooses Personal Learner Record as evidence they would like to use to (instead of passport).
    e. User goes through Knowledge Based Verification (KBV). The questions are based on the information gleaned from their Personal Learner Record.
    f. User successfully registers with the IdP

   User journey 2 (in practise extension of UJ 1):
    a. After successfully registering with the Identity Provider (as per the above), User is given an option of downloading a document containing Personal Learner Record.
    b. User is then redirected back to the Service Provider and continues with original task of applying for a provisional driving licence.

   User journey 3:
    a. User is applying for a provisional driving licence online.
    b. User is redirected from the service provider to GOV.UK Verify to register with one of the Identity Providers.
    c. User chooses one of the Identity Providers to register with.
    d. User, at the Identity Provider's home screen, clicks the option of Personal Data Store (PDS) (that they have one)
    e. User is redirected to their PDS and sign in
    f. User is asked to select evidence from the documents they have stored in their PDS they would like to share in order to get their identity verified.
    g. User then returns to the IdP and is successfully verified
    h. User is redirected back to the Service Provider and continues with original task of applying for a provisional driving licence.

DSOT 2 User journeys:

1. User journey 1:
    a. User (a selected number of students from a college) receives Enrolment Letter with QR code on it.
    b. User goes into a face to face meeting with an organisation in order to open an account and prove their identity.
    c. User presents evidence, including the enrolment letter with a QR code, as part of the registration.
    d. Individual processing the registration scans the QR code from the letter with a device (mobile phone) and checks the information that comes up on the screen against the information on the letter.

e. User continues with registration.
f. User successfully opens an account.

1. User journey 2 (secondary journey):
   a. User (existing member of the organisation) receives a paying-in book with a QR code on it.
   b. User goes into a branch of the organisation and presents the QR code on the paying-in book to the cashier.
   c. User is able to see their account balance on the screen of a device provided by the organisation.

Appendix B

Learnings, Benefits and Barriers of applying these methods

Learnings:

- User research highlighted the need for processes that will facilitate thin file cohort's verification of their identity.
- The use of QR codes in both onboarding of new members and an existing member transaction, at South Yorkshire Credit Union, was seen as very efficient and easy. Currently, the South Yorkshire Credit Union onboarding process is lengthy as KYC checks the South Yorkshire Credit Union does are more involved than a traditional high street bank or financial institution. This is because the South Yorkshire Credit Union has to use a broader range of documents for this particular demographic, and checks the validity of these documents with the issuing source. This can be time consuming and take up to 20 minutes to complete. The use of QR codes gave the South Yorkshire Credit Union greater confidence in the document itself and the information on it, when checked against the digital data associated with the QR code. The letter from the college scoring 2 in the IPV Element B 26, while the South Yorkshire Credit Union pay in book scored 3.
- The South Yorkshire Credit Union believes this type of process would allow them (or other relying parties with similar issues) to speed up verification of one's identity and document validity checks as well as enhance the services offered to the members such as meet and greet activities in branch. It would also encourage take-up and adoption of remote service access across different channels/devices
- Technology acceptance and usability: One of the worries was how users would perceive the technology used, and paper documents having a digital presence used to validate the authenticity of those documents that would also include their photo. While there wasn't great interaction between the user and the QR code itself, the end result produced by this technology was perceived very positively by the user. The fact they could use a paper document to prove who they say they are (and additionally this being linked to their photo) was very well received by the users. Also use of popular/familiar technologies such as PDFs and QR codes facilitates the adoption through familiar interfaces and tools.
- One of the key learnings for the Digital Notary Service Provider was that there was no need for the service to hold the data about the users. The design where the service acts essentially as an enabler/route

between a relying party and issuing authority works very well. It eliminates creation of a central database of attributes and aligns with a federated model approach taken by IDAP. It also provides validation at source.

- People recognise the value of having their identity validated online. With social networks being very common among different demographics, they become aware of the fact they need to authenticate to sign-in to their personal profiles and accounts.
- Thin-file citizens will have a hard time proving their identity online. Their inability to have the identity validated online potentially excludes them from access to core public and private sector services. This means that any progress in facilitating their journey will be well-received.
- Few people are aware of concepts like a Personal Data Store, but when explained they understand the value of a cloud service holding documents and data about themselves under their full control.

Benefits:

- Access to additional/new services - by providing evidence in digital format which allows users to create digital identity with Identity Providers, users would be able to reuse this identity across other services available through GOV.UK Verify. The plan is to increase number of public services that use GOV.UK Verify. The long run vision is to also allow reuse of the digital identity in the private sector.
- Convenience - Thin file cohort faces challenges of proving they are who they say they are on a daily basis. At present applying for various services is very complex, if not impossible due to their lack of appropriate identity documents. By developing user journey(s) across services described in the two projects users would gain more convenient access to various services. This would be true of both public and private sector services.
- Time saving - All journeys explored are likely to offer time saving to the user.
- Potential commercial opportunity for Issuing Authorities.
- Time savings when Issuing Authorities are asked to validate their customers by other organisations.
- Ability to repudiate documents Issuing Authorities have issued.
- Better all round service and customer experience for Relying Parties.
- Eventual ease of acceptance, access and use of electronic services for self-service, as well as improvement of face-to-face process for Relying Parties.
- Relying Parties having a greater level of assurance around document validity and thus reducing potential risk of fraud (the regulating authority, the Prudential Regulation Authority does not underwrite such fraud if the account documentation is proven to be forged or incorrect).
- Potential cost savings for Relying Parties.
- Reduced staff time performing critical and accurate identity and document validity checks.

- Doing this to recognised and agreed Government standards set in the GPGs, will ensure that as new services (from possibly new partners) become available that they can be easily accessed, assimilated and applied.
- Potential opportunity for the South Yorkshire Credit Union where public, third and private sector organisation could make use of the transferable, highly credited South Yorkshire Credit Union's 'trust' network.
- Introduction of a new service by private sector (attribute gateway or digital notary services).
- Participants' view of the ease of use of such services.
- Identity Assurance Programme is an opportunity for the digital innovation of public services (i.e. adoption of digital communication means with citizen and business in place of paper-based communications). This turns into immediate advantage in terms of cost reduction, speed, security, fraud prevention, and finally re-use of information.
- There are many data items available from Issuing Authorities (Government Agencies, Schools) which could be used as part of a validation process by Identity Providers. These data can be turned into secure digital documents and turned at the same time into structured metadata inside them and then delivered to citizen and serve as a new digital source of evidence to perform identity checks.
- Storing documents into PDS would allow to quickly access them from anywhere, anytime and from any device (including smartphones) and would also allow to vouch third parties to have limited and controlled access to these documents and their metadata, such as in the case of Identity Provider when required to validate the citizen's identity online.
- Utilisation of DRM provides an easy, yet secure way to distribute sensitive information to citizens, service members, or other users via web or mobile sites. It enables the creation of personalised PDF documents that are more secure than paper and allow desktop or mobile users to access them via a website or web portal. Document security encrypts files and applies persistent and dynamic policies that help maintain confidentiality and control use on fixed or mobile devices. Usage rights can be changed for a user or group, even after a file is distributed.

Barriers:

- Potential cost of the types of services explored in the projects - the cost of the services has not been discussed in the projects and would have to be explored independently between the providers and the Relying Parties/Identity Providers.
- Potential miscommunication with users and thus rejection of the service.
- Getting agreements of data access and the sharing of data with the various service providers.
- Lack of uptake from Issuing Authorities and Relying Parties.
- People have different sensitivities to data sourced from their citizenship, financial transactions, personal/social profiles. Identity Providers should be able to offer a breadth of choice when using

knowledge-based verification to perform their check to avoid citizens experiencing a sense of loss of control of their sensitive information.

- Some people have limited knowledge of existing data and documents on their account. They are more inclined to share information from sources and documents they know well rather than from unknown sources.
- Moving from small-scale to large-scale services.

Appendix C

The workflows used by the Digital Notary Service Provider are described below:

The Issuing Authority:

- Produces the Digests of the Identity Evidence detailed on the document
- Produces a QR Code and sends data to the Authoritative Source which is cryptographically signed
  - At a minimum the data includes the digests of the Identity Evidence
  - The data may include cryptographically encoded data that includes such things as photographs which are too large to fit on the QR Code
- Prints or otherwise attaches the QR Code to the document

Relying Party

- The QR code (cryptographic key) is scanned
- The data in the QR code, and the data held by the Authoritative Source are combined
- The combined data produces Identity Evidence i.e. the Personal Details of the citizen. This may include a photo/image of the person to whom it was issued.
- The resulting Identity Evidence can be checked by the Identity Provider to verify that it was cryptographically signed by the Issuing Authority, and Genuine

The Validoc approach tested in 'Digital Sources of Trust 2' is very simple. In summary the QR code on the document when combined with data on the Authoritative Source server verifies the authorship and contents of the documents in a way that is compatible with GPG 45.

Features of the Solution

The Cryptographic Signature

All the data that is sent to the Authoritative Source server, by the Issuing Authority, has to be signed by a cryptographic signature: the x.509 private key of the Issuing Authority. This uses the internationally recognised infrastructure that powers most of the commercial internet. It is often called an "SSL certificate", and almost every web transaction uses these.

The power of the cryptographic signature is that a third party (such as an IdP) can verify that the author of the document was in fact the Issuing Authority, without worrying about the security or robustness of the Authoritative Source service. The Authoritative Source does not have the capability to manipulate, in anything other than a destructive way, the data provided by the Issuing Authority. So for example it could corrupt (in an obvious way) or delete the Identity Evidence, but not insert or edit Identity Evidence.

Digests

There is an ancillary problem that has to be dealt with. Not in order to meet the Good Practice Guidelines, but instead to ensure that Issuing Authorities can engage with the programme easily.

Much of this Identity Evidence is either commercially sensitive or subject to the data protection act. Encouraging Issuing Authorities to hand this Identity Evidence to a third party Authoritative Source is a long and complex process. However by only requiring the Issuing Authority to send the digests of the data, the Authoritative Source does not have access to the actual data, and many of the concerns vanish.

Destale-ing of documents

Because the physical documents now in effect have an electronic presence, when the one hundred and eighty day check is required, it may be possible in some cases to have a fully automated re-verification of identity.

For example suppose one of the supporting documents was a gas bill, and that the citizen has been receiving gas bills from the same supplier for the intervening six months. When it is time to review their identity, the Authoritative Source will be able to assert that the address has not changed in the last six months: as the digests will not have changed. This effectively means that a document that was used as proof of address six months ago, has been 'refreshed'.

Glossary

Term	Definition
Attribute	A piece of information or data that is associated with an identity.
Digital Rights Management (DRM)	A set of access control technologies used to protect the confidentiality of digital documents, information and contents.
Genuine	To be what something is said to be; i.e. authentic not counterfeit.
Identity	A collection of attributes that uniquely define a person or organisation. The fact of being whom or what a person or thing is.
Identity Provider (IdP)	A trusted organisation that verifies an individual identity according to agreed standards.
Issuing Authority	An authority that is responsible for the generation of data and/or documents that can be used as identity evidence.
Know Your Customer (KYC) checks	KYC is the due diligence and regulation that financial institutions and regulated companies must perform in order to identify their clients. Relevant information needs also to be identified in order for those organisations to do financial business with them.
Knowledge Based Verification (KBV)	Static Where a secret has been previously exchanged between two parties. One party uses the secret to verify that they are the other party with whom the secret was originally exchanged. Also referred to as a *shared secret.* Dynamic A process where the applicant is required to provide answers to questions relating to the claimed identity.
Levels of Assurance (LoAs)	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. There are four LoAs under CO's GPG45
Metadata	Data about data, or information known about an object in order to provide access to the object. Usually includes information about intellectual content, digital representation data, and security or rights management information.
Personal Data Store (PDS)	A personal proof bank for individuals to store identity documents and manage how they are accessed by others. An example is that offered by MyDex.
Personal Learning Record (PLR)	"Your Personal Learning Record is a place where you can store and view all your learning achievements. We automatically add details of courses you've recently completed (starting from the 2007/08 academic year) or are currently doing with a recognised learning provider. This includes courses from school and further education, but not higher education. You can also add course details yourself."

	source: https://nationalcareersservice.direct.gov.uk/tools/learn/Pages/whatisaPersonalLearningRecord.aspx
Relying Party (RP)	The party in a transaction that relies upon an assertion, such as identity details, from another party.
Thin-file citizens	Defined here as those lacking formal identity documents such as passport, driving licence, birth certificate, documents typically required to get someone to a level of assurance where an organisation will be willing to provide a service, e.g. a bank.
Valid	To know that something stated is true.