OIX OPEN IDENTITY EXCHANGE White Paper

USING GOV.UK VERIFY FOR LOCAL AUTHORITY MULTI SERVICE PORTALS (ALPHA PROJECT)

WHITE PAPER

Ian Litton

November 2018

etive TECHNOLOGIES

EXECUTIVE SUMMARY

> *"This project is exciting for Post Office in being able to demonstrate the use of Verify. Supporting more customers by diversifying the range of data sources available to meet high government standards of identity assurance. It is important to make proving identity easier for those with thin credit files, whilst retaining robust and appropriate checks to prevent identity fraud. Doing this will simplify how customers transact digitally with local authorities and housing associations, improving the process for everyone."*
> *Post Office*

Federated identity is a powerful mechanism for increasing customer convenience, enhancing organisational efficiency and transforming the way online services are delivered.

In the UK there is currently only one federated identity solution that offers highly assured customer identities backed up by clear, agreed standards. That solution is GOV.UK Verify.

The GOV.UK Verify registration is designed as a fully online process. Although this offers undeniable benefits, there is a significant cohort of thin-file customers who may not have any, or a sufficient digital footprint in commercially available data sources to meet the government standard for GOV.UK Verify registration.

This Alpha project, building on an OIX Discovery project[1], demonstrates how the use of data collected by local authorities (LAs), made available to identity providers (IDPs), could help otherwise thin-file customers register for a GOV.UK Verify identity.

We demonstrate that LAs have sufficiently robust information governance processes in place to be able to provide quality data to IDPs for identity proofing and verification under the Verify scheme, and that this data would be sufficient to help the majority of thin-file customers achieve a Verify account at level of assurance 2 (LOA2).

We show that there is a strong business case for LAs to adopt GOV.UK Verify, and that there is also a business case for IDPs to use LA data in the identity proofing and verification process.

Based on consultations conducted with LAs and IT suppliers to the LA market, we recommend how Verify should develop in order to better serve the LA market. We have also developed an example customer journey, based on those consultations, and produced a high-level technical solution.

---

[1] See https://oixuk.org/wp-content/uploads/2017/02/Micro-Sources-of-Data-Final-.pdf

We conclude that LA data provides a valuable and practical solution to making GOV.UK Verify available to the widest range of potential customers, and that a Beta project should be set up to demonstrate this in practice, and to stimulate the LA market for GOV.UK Verify. The recently signed contracts between government and 5 IDPs present the perfect opportunity to achieve this, as the changes broaden the use of Verify and identity standards beyond public sector, a key aspect for a successful identity assurance scheme, in a way that also better meets the needs of LAs.

INTRODUCTION

This White Paper describes how data collected locally, by local authorities (LAs), housing associations (HAs) and similar organisations, could be used to extend the reach of GOV.UK Verify. In particular this paper addresses the needs of "thin-file" customers who may not have any, or sufficient digital footprint in commercially available data sources to meet the government standard for identity proofing and verification as implemented by GOV.UK Verify. These people are often the heaviest users of public services who would benefit most from transacting online. LAs could achieve significant savings if this cohort were able to transact digitally.

The thin-file cohort is a significant problem in the context of GOV.UK Verify. Three of the key sources of data available to Verify IDPs are UK passports, UK driving licences, and credit reference data. The following table highlights the penetration of passports, driving licences and credit cards for the general population compared to those on Jobseeker's Allowance (JSA):

	General Population	JSA
Passport	80%	64%
Photo Driving Licence	75%	52%
Credit Card	56%	31%

Table 1. Penetration of passports, driving licences and credit cards for the general population compared to those on Jobseeker's Allowance (JSA)

People on JSA are significantly less likely to have these key pieces of evidence.

As a result, there are key cohorts of citizens who are unable to successfully register with a GOV.UK Verify IDP. These citizens are typically the people who are the heaviest users of public services, for whom the benefits of transacting online would be the greatest.

This problem has been highlighted recently in relation to Universal Credit. Only 38% of Universal Credit claimants who attempt to use GOV.UK Verify manage to register successfully[2]. This comes at a cost too. The Department for Work and Pensions (DWP)

[2] See the NAO report on Rolling Out Universal Credit, section 3.21: https://www.nao.org.uk/wp-content/uploads/2018/06/Rolling-out-Universal-Credit.pdf. See also the November 2017 minutes of the

estimates that the manual identity checks that will be necessary as a result of low registration rates will reduce their potential savings from the roll-out of GOV.UK Verify by £40m over 10 years.

To address this "hard to verify" or "thin-file" cohort, it is essential to make a wider range of data sources, covering different types of data, available to the GOV.UK Verify IDPs. This White Paper demonstrates that LAs are a valuable and practical source of such data. It also demonstrates that there is a compelling business case for local authorities and other organisations to adopt a federated citizen identity solution to meet their strategic objectives of delivering services more effectively, efficiently, and cheaply through online channels.

Federated identity is a powerful mechanism for increasing customer convenience, enhancing organisational efficiency and transforming the way online services are delivered. Built to agreed, interoperable standards, a federated identity system can deliver a range of benefits:

- a customer centric identity that can give access to a wide range of services across the public and private sectors;
- shared trust, facilitating access to a wide range of attributes for a relying party to establish customer entitlement and eligibility, with customer permission;
- increased security and reduced levels of fraud;
- financial savings for organisations and their customers;
- increased convenience and reduced transaction friction for organisations and customers.

Without a federated citizen identity solution delivering high levels of assurance and trust, it is impossible to achieve full end to end digital transformation of higher risk services and of more complex services that require eligibility checks. Eligibility checking, using attribute exchange, requires a shared trust anchor for identity, which a federated system provides.

In the UK there is currently only one federated identity scheme that is capable of delivering the necessary high level of trust, based on an agreed set of standards, that can deliver all of the benefits outlined above. That scheme is GOV.UK Verify.

It is an exciting time in the evolution of GOV.UK Verify. In May 2018 the Government Digital Service (GDS) announced their intention to support the roll out of high-level

---

Privacy and Consumer Advisory Group meeting, item 3. Even with support, only 1 in 5 people were able to verify their identity in a trial carried out in Croydon.

government standards for identity proofing and verification into the private sector and to continue to support development of an identity market in the UK that leads to the creation of ubiquitous digital identity. In October 2018 5 IDPs entered into new contracts with Government to enable this development. This provides an ideal opportunity to extend the reach of GOV.UK Verify, but also to explore how GOV.UK Verify might evolve to better meet the market needs for federated identity. This White Paper feeds in to that debate.

The hypothesis we set out to investigate in this project is that local authority transaction data could be used by IDPs to raise the level of assurance of a thin-file customer's digital identity, and enable nearly all local authority customers to take advantage of GOV.UK Verify.

The project objectives were to:

1. develop an example service, delivered through the Etive Digital Log Book (DLB), incorporating GOV.UK Verify;
2. demonstrate how data in the DLB could, with the user's consent, be passed to an IDP in order to elevate the level of assurance associated with that user's GOV.UK Verify identity;
3. design a technical architecture that enables the above;
4. address the data governance issues raised in the previous Etive OIX Discovery Project[3] and to confirm that:
    a. the processes and procedures used by the local authorities to on-board their customers are sufficiently robust to provide reliable identity evidence to IDPs;
    b. the evidence available meets the requirements set out in the Government's Good Practice Guides for identity proofing and verification;
    c. the evidence available usefully covers the evidence categories currently lacking for the hard to reach client group in question;
5. prepare a business case to demonstrate the value that local authorities and other relying parties could derive from their customers having a GOV.UK Verify account, and the value IDPs could derive from access to LA data;
6. communicate the project findings to LAs and their IT suppliers to help speed up the understanding and adoption of GOV.UK Verify.

[3] https://oixuk.org/wp-content/uploads/2017/02/Micro-Sources-of-Data-Final-.pdf

PROJECT DESIGN

There were 3 main project streams:

1. **Information Governance** - assessing the quality of local processes and data, and how well they measure up to the requirements of Good Practice Guide 45[4];
2. **Business Case** - the benefits of adopting GOV.UK Verify as a federated citizen identity solution for LA services;
3. **Industry Consultation** - raising supplier and local authority awareness and understanding of GOV.UK Verify, and gaining feedback from the sector.

Each of these work streams is described in the sections below.

We also modelled an example customer journey, and drafted a technical solution.

In the course of this project it became clear that to meet the needs of LAs and HAs, GOV.UK Verify needs to evolve. We highlight how GOV.UK Verify needs to change to become a more complete solution.

We conclude with recommendations for next steps.

A range of stakeholders were involved in the work streams, including LAs and representative bodies, IDPs, a hub provider, IT suppliers to the LA market, and GDS. The participants and the roles they performed in the project are listed in Appendix A

WORK STREAM 1 - INFORMATION GOVERNANCE

An earlier OIX Discovery project described how LA data could be used by GOV.UK Verify IDPs to improve registration rates for thin-file customers. The Alpha project established that the data collection processes in our participating LAs were robust and would meet the standards set out in the Government's Good Practice Guide 45 for data sources used for identity proofing and verification.

INFORMATION GOVERNANCE APPROACH

An information compliance audit was conducted with the London Boroughs of Tower Hamlets (LBTH) and Hackney (LBH) to review how they carry out identity proofing and verification at present in the context of applications to their social housing registers, and how this matches up to the requirements of Good Practice Guide 45 - "Identity proofing and verification of an individual".

[4] See https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual

Each council's written procedures were reviewed. We also observed how the procedures were implemented in the one stop shops and back-office operations dealing with social housing applications. From this engagement with the councils we developed ideas on how a self-certification process might work for local sources of data.

An industry consultation event on information governance was held in relation to identity proofing and verification. From this an information compliance report was produced and reviewed by GDS and two of the project IdPs. The full information compliance report is available on the OIX website[5].

INFORMATION GOVERNANCE FINDINGS

The key findings from the Information Governance work are that:

1. the processes documented and observed are capable of providing a comprehensive data source for GOV.UK Verify IDPs;
2. there is sufficient evidence against the Identity Proofing and Verification (IPV) elements A, B and C, and, for some applicants, IPV-E, to help achieve an LOA2 Identity [6];
3. the processes undertaken capture data in a manner consistent with a rating of "strong" for the purposes of use by an IDP to create an LOA2 identity, with the addition of the IDP's access to IPV-D required material, such as Deaths, National Change of Address register (NCOA), Politically Exposed Persons register (PEPS , Sanctions and Fraud;
4. the data being collected by the London Boroughs of Tower Hamlets and Hackney, and the processes involved in capturing that data, are of sufficient quality to be used in the identity proofing and verification undertaken by Identity Providers within the GOV.UK Verify scheme.

A key finding of this project stream is that the LAs observed meet the necessary data and process standards required to support GOV.UK Verify identity proofing and verification. These observations relate to social housing transactions, but it is likely that other local authority processes, for example financial assessments for social care, would

[5] https://oixuk.org/blog/2018/11/23/using-gov-uk-verify-for-local-authority-multi-service-portals-alpha-project/

[6] IPV-A relates to the strength of the identity evidence presented; IPV-B relates to the validation of the identity evidence - is it genuine? IPV-C relates to the verification of the identity evidence - does it belong to the person who claims it? IPV-D relates to counter fraud measures associated with the identity. IPV-E relates to activity history associated with the identity.

also provide data of high value in the identity proofing and verification process, although in lower volumes.

A self-certification process could be developed to help LAs assess if they meet the necessary standards to provide data into the GOV.UK Verify identity proofing and verification process. This self-certification scheme would cover the following areas:

Written procedures	Does the organisation have formal written procedures for ID verification? How are these signed off? What is the review process?
Staff training	What training do staff receive in identity proofing and verification, in document checking, and in anti-fraud procedures? Is regular refresher training delivered?
Documents accepted as proof of identity and eligibility	Does the range of documents that must be presented match the requirement of GPG 45?
Policy on original documents	Which documents must be presented in their original format; when are copies/prints from the internet accepted?
Use of scanning devices	Are scanning devices used to detect fraudulent documents? If so, in what circumstances?
Counter fraud measures	What counter fraud measures are deployed e.g. credit record agency checks, other cross checks?
Quality assurance processes	Do supervisors carry out cross-checks and spot checks to ensure processes are being followed correctly?
Face to face checks	Are face to face checks carried out to link individuals to asserted documents (passports, driving licences etc)?

Cross checking	What cross-checks are made between different document types e.g. benefit payments into the bank account match the benefit awards notice?
Relevant accreditations	For example, the level achieved against the Information Governance Toolkit / Data Security and Protection Toolkit

Table 2. Potential elements of a self-certification process for micro-sources of identity data

These ideas would be developed further in a subsequent Beta project, but related industry sectors already have experience of self-certification (e.g. the OpenID Certification Program, the OIXnet Registry, and tScheme) from which we can learn lessons in terms of legal, technical, and registration approaches.

It is likely that the provision of LA data into the Verify identity proofing and verification process would be covered by contractual arrangements with the IDPs, to ensure the necessary information governance standards were in force at the LA.

In summary, the Alpha project confirms that locally collected data is suitable to be used in the GOV.UK Verify identity proofing and verification process.

WORK STREAM 2 - BUSINESS CASE

The core of this Alpha project is exploring how locally held data can help thin-file users verify themselves through GOV.UK Verify IDPs. It is important to take a step back, though, and explore why highly assured online identity makes business sense. What is in it for local authorities, their partners and their customers? What is in it for IDPs? What additional benefit does the Etive Digital Log Book confer? In short, what is the business case for using a federated approach to identity, and a personal data store?

The business case is explained in more detail in a separate business case document, also available on the OIX website[7]. In the following sections we describe our overall approach and highlight the main findings.

BUSINESS CASE APPROACH

[7] https://oixuk.org/blog/2018/11/23/using-gov-uk-verify-for-local-authority-multi-service-portals-alpha-project/

To produce a business case, we worked with two local authority partners, the London Boroughs of Tower Hamlets and Hackney, with the Greater London Authority (GLA), the Post Office, and GDS. We also ran an industry consultation event to gather input from LA suppliers.

The business case covers the following areas:

1. **indicative overall benefits.** We have been able to reference previous research carried out as part of the #VerifyLocal pilots run by GDS with a dozen local authorities. This research has been built into a Local Verify Benefits Calculator tool[8] that embeds some generic metrics, and can be configured by local authorities to give an indication of the scale of benefit they might derive from GOV.UK Verify. This tool is described in more detail in the separate Business Case document, but the headline figures referenced in the next section relate to an example metropolitan council with 275,000 residents, delivering the full set of local government services;
2. **social housing.** We have explored social housing transactions in more detail and demonstrate that the benefits identified in the Local Verify Benefits Calculator are likely to be conservative. Social housing is one of the more complex services, requiring more rigorous identity and eligibility checks;
3. **federated identity.** We explore the particular benefits that accrue from adopting a federated solution to identity, with particular reference to population churn in metropolitan areas, multi-agency working, and vulnerable groups such as the homeless;
4. **fraud.** We refer to existing government and industry research to indicate the amount of fraud-related cost our example metropolitan council with 275,000 residents might avoid;
5. **systems integration.** Through our industry consultation we have begun to understand the integration costs that could be reduced if the sector as a whole were to adopt a common approach to federated identity;
6. **value of local data.** By providing validated and verified data into the identity proofing and verification process, local authorities and housing associations would become active partners in identity proofing and verification, rather than passive recipients of identities. This data would have value, and could offset the cost to the relying parties of identity proofing and verification. We have also identified how this data could help the GOV.UK Verify IDPs deliver highly assured identities to thin-file customers who do not have any, or a sufficient digital footprint in commercially available data sources to meet the government standard for GOV.UK Verify registration

[8] https://oixuk.org/blog/2018/11/23/using-gov-uk-verify-for-local-authority-multi-service-portals-alpha-project/

7. **personal data stores.** We explore the additional benefits that can accrue from including a personal data store, such as the Etive Digital Log Book, as part of a federated identity solution.

THE NEED FOR AN ECOSYSTEMS APPROACH

Assured online identity is a prerequisite for delivering higher risk services online, i.e. services that deliver benefits in cash or kind, or that share sensitive personal information with users.

Fully digital end-to-end service transformation relies on more than just an assured online identity. For 81 local authority services proof of eligibility is also required. Establishing eligibility without recourse to expensive, slow and inconvenient paper processes requires an additional, but linked, ecosystem - the attribute exchange ecosystem. Attribute exchange is described in more detail in the separate Business Case paper[9].

The potential cost savings that could be made by adopting attribute exchange are built into the business case, and to the Local Verify Benefits Calculator. The benefit of GOV.UK Verify will be magnified when the identity ecosystem is paired with an attribute exchange ecosystem. Attribute exchange helps deliver a compelling business case for adopting GOV.UK Verify in the first place[10].

BUSINESS CASE RESULTS

The headline figures given below are described in more detail in the separate Business Case document[11].

An example metropolitan council with 275,000 residents, delivering the full range of local government services could save **£16.78m** over a five-year period by transforming their services with GOV.UK Verify and attribute exchange. This figure is made up of:

A. **£4.45m** identity assurance savings
B. **£2.50m** eligibility checking savings
C. **£9.83m** service delivery savings

[9] https://oixuk.org/blog/2018/11/23/using-gov-uk-verify-for-local-authority-multi-service-portals-alpha-project/

[10] The role to be played by attribute exchange has recently been emphasised by the Chief Digital Officer at MHCLG. See http://www.ukauthority.com/data4good/entry/8228/mhclg-digital-chief-points-to-attribute-exchange-potential

[11] https://oixuk.org/blog/2018/11/23/using-gov-uk-verify-for-local-authority-multi-service-portals-alpha-project/

Year-on-year savings after the 5-year implementation period, for the example council, could amount to **£4.435m**.

The generic metrics used in the model that generate these savings figures yield an estimated cost per case for social housing transactions is **£10.87**. However, research with one local authority showed their costs to be closer to **£350** per case. Although we need to validate this social housing figure by comparison with other local authorities, it does indicate that the benefits figures yielded by the Local Verify Benefits Calculator are likely to be conservative rather than optimistic.

We estimate that the example metropolitan council of 275,000 residents could also avoid fraud losses of **£4.7m** over the 5-year implementation period by adopting GOV.UK Verify.

A common approach to federated identity, based on GOV.UK Verify, could save between **£412k** and **£1.24m** per annum in London alone by avoiding the need to re-register citizens every time they move. This is based on population churn figures for London. In 2016 317,000 people over the age of 18 moved from one London borough to another. The benefits to be derived from adopting a federated approach to identity for the "hard to verify" would be proportionally greater, given the additional effort required to register this cohort in the first place. Similar benefits, albeit smaller in volume, are likely to accrue in any metropolitan area.

Access to a federated identity is of particular value to vulnerable groups, such as the homeless and victims of domestic abuse, who are more likely to lose or be separated from their identity documents or to have them stolen. Replacement documents can be expensive, and the cost of replacement often falls to the third sector. Example replacement costs are:

A. Birth certificate **£9.50**

B. EU passports/ID cards **£21.60** to **£104.60**

C. Replacement Biometric Residence Permit **£56**

D. Confirmation of Indefinite Leave to Remain **£237**

While replacement documents are being sought these vulnerable users are also unable to access the services they need.

A top-5 supplier to local authorities estimated that a lack of standards for identity across local authority systems could lead to systems integration costs of **£50m** for local authority suppliers, for identities at LOA1. Additional cost would be incurred for LOA2

accounts. Standardising on GOV.UK Verify would reduce this cost, and integration time, by providing a common interface and approach.

Local organisations who are actively engaged in helping customers prove who they are should benefit from reduced identity proofing and verification charges in recognition of the value they are adding to the process. We have not attempted to quantify the potential savings, or to suggest particular commercial models in this project, but recognise this is one of the key topics that will have to be addressed.

Apart from acting as a store of valuable identity evidence, a personal data store can store other credentials and evidence that the user can choose to share with different service providers, as the need arises. Citizens can share their data with chosen organisations, for a limited period of time, and for specific purposes. This can be particularly useful for users who are highly mobile, or who have to deal with multiple agencies in order to get a job done. It can be invaluable for vulnerable groups, such as the homeless and victims of domestic abuse, who are more likely to lose identity documents, have them stolen, or be separated from them. The separate Business Case document discusses some potential use cases.

A personal data store also allows identity proofing and verification to become a process over time, rather than a point in time pass/fail exercise. As more identity-related information is collected in a personal data store, the opportunity for the user to reach a higher level of assurance through their IDP increases.

For IDPs, there are benefits in being able to successfully offer highly assured identity services to a wider range of customers, including currently thin-file customers. Research carried out in Tower Hamlets in relation to their WorkPath service (a service that helps local residents find and stay in work), indicate that 98% of that cohort would have sufficiently strong evidence to achieve an LOA2 identity verification. 89% of the cohort (including 19% from overseas) would have strong photo-id, allowing for strong ID verification. 63% of the cohort are likely to have sufficient activity history to achieve LOA2. The DLB would provide the rest the opportunity to build up activity history over time. Opening up the LA market in general to GOV.UK Verify has the potential to significantly extend the reach of GOV.UK Verify to many more customers, which would provide IDPs with a significant market opportunity.

The evidence we have assembled demonstrates that local authorities and other organisations could derive significant benefits, quantitative and qualitative, by adopting GOV.UK Verify.

WORK STREAM 3 - INDUSTRY CONSULTATION

As part of the project we engaged with IT suppliers to the LA sector. This was partly to make suppliers aware of the benefits of a federated approach to identity, to raise

awareness of GOV.UK Verify in particular, and explain the link between federated identity and attribute exchange. Combined with this, we felt it was important to get their input into the solutions being developed, due to their role as major suppliers to local authorities. From the consultations we formulated ideas on how GOV.UK Verify should evolve to better serve the LA market.

CONSULTATION APPROACH

We partnered with techUK to run four consultation events. Suppliers to the local authority market were invited to attend. A list of the organisations who attended these consultations is shown in appendix C[12].

Consultation 1 introduced the benefits of GOV.UK Verify and gave an overview of the project. Round table sessions were set up to cover: using local data in identity proofing and verification; user interface issues; the business case for GOV.UK Verify in local authorities; the local authority market for GOV.UK Verify; and private sector hubs.

Consultation 2 went into more detail about how GOV.UK Verify identity proofing and verification works and discussed the information governance workstream, and technical design.

Consultation 3 dealt with user interface and design.

Consultation 4 summarised the project findings.

Input from delegates was actively sought in all 4 workshops, which was then followed up with one-to-one discussions with some of the suppliers.

CONSULTATION OUTCOMES

The consultation events provided useful feedback on all aspects of the project. Some clear messages emerged from the engagement with LAs and suppliers on how GOV.UK Verify should evolve.

The key features of the modified GOV.UK Verify model we are proposing are:

1. an ecosystems approach;
2. full federation across all levels of assurance;
3. using local data in the identity proofing and verification process;

[12] Please note that attendance does not necessarily mean endorsement of views expressed in the paper

4. allowing relying parties to offer a single IDP when registering new users;
5. different commercial models.

AN ECOSYSTEMS APPROACH.

An ecosystems approach would combine attribute exchange with GOV.UK Verify identities to achieve full value from digital identity. A consistent message from all the local authorities and suppliers we have spoken to is that attribute exchange delivers the real business case for adopting federated identity. There is growing recognition in government too that attribute exchange is essential to fundamentally transform the way services are delivered online[13]. Attributes need to flow between the public and private sectors, not just within the public sector, so the adoption of a common standard for identity across the public and private sectors is absolutely necessary to deliver the levels of trust required for data to flow effectively, securely, and in line with customer preferences. A standards-based approach to attribute exchange is equally necessary.

There may be other technical implications for GOV.UK Verify in adopting an ecosystems approach. For example, the ability to maintain session state[14] for identity sessions would allow attribute providers to confirm that a citizen has logged in at the required level of assurance to permit the release of attributes.

FULL FEDERATION AT ALL LEVELS OF ASSURANCE

Many local authorities currently offer their citizens "My Account" facilities at low levels of assurance that allow customers to log in, pre-populate online forms, save forms, track call progress and so on. These types of accounts are perfectly adequate for low-risk transactions where the customer's identity does not need to be confirmed. Simple login accounts are not currently offered by GOV.UK Verify. This leaves local authorities with a number of choices:

1. to run their own simple login "My Account" in parallel with GOV.UK Verify. This is not a good use of resources and creates an issue for customers who later want and need to elevate the level of assurance associated with their online identity;
2. to force customers to register for a GOV.UK Verify account at LOA1 when it is not strictly necessary. This introduces unnecessary friction, and potentially cost, into the online process;
3. for LAs to develop their own solutions to LOA1 and LOA2 accounts, which is complex, expensive, and defeats the benefits of a platform approach across the

[13] See http://www.ukauthority.com/data4good/entry/8228/mhclg-digital-chief-points-to-attribute-exchange-potential and https://dwpdigital.blog.gov.uk/2017/09/19/helping-citizens-choose-how-their-data-can-work-for-them/

14 Stateful means the computer or program keeps track of the state of an interaction over time.

public sector. Locally developed LOA1 and LOA2 accounts are also very unlikely to deliver the levels of trust required to support the attribute exchange ecosystem.

Local authorities need to have the choice to fully outsource their citizen identity solution to GOV.UK Verify IDPs, and for those solutions to cover the full range of levels of assurance. Citizens can be given the option to elevate the level of assurance associated with their online identity as the need arises. As we have shown in initial user interface designs (see appendix B), there is also the option to engineer a customer journey so that the customer can get on with the job in hand with minimum friction by creating a simple login, and then increase the assurance associated with their online identity at the point in the process when it is required.

USING LOCAL DATA IN THE IDENTITY PROOFING AND VERIFICATION PROCESS

Additional data sources can be, and have been, brought on stream in the past to help the GOV.UK Verify IDPs improve their identity proofing and verification processes. This project has demonstrated the enormous potential of allowing local authority data to be added to the list of available data sources. The face-to-face processes already in place in local authorities, and the cross-checks they carry out to ensure applicants are entitled to key services, make this data particularly valuable in enabling people, who are currently hard to verify, to get an identity account with a GOV.UK Verify IDP. We believe that the outcomes from this project demonstrate that local authority data, properly accredited, should become part of the GOV.UK Verify identity proofing and verification processes carried out by IDPs.

Of course, there is data in other parts of government, and in the private sector, that could be equally valuable in improving the success rate of GOV.UK Verify registrations. DWP and HMRC data, for example, could also help the currently hard to verify achieve a GOV.UK Verify account. We would strongly recommend research into the feasibility of bringing additional data into the identity proofing and verification process.

CONTRACTING WITH A SINGLE IDP

Allowing relying parties to offer a single IDP when registering new users for a GOV.UK Verify ID would remove significant complexity from the user journey. Having to choose an IDP from the 5 on offer is one of the more difficult aspects of the GOV.UK Verify user journey. Offering a single IDP has a valuable role to play in reducing friction in the registration process.

Offering a single IDP would also give relying parties the opportunity to negotiate favourable commercial terms with their chosen IDP. These commercial terms could include recompense to the relying party for providing data into the identity proofing and verification process. User choice can still prevail in this environment, as customers could reuse Verify IDs already registered with another IDP in the context of transactions with other relying parties. Indeed, the opportunities to do so will only increase as GOV.UK Verify is rolled out across the private sector.

DIFFERENT COMMERCIAL MODELS

GOV.UK Verify offers a single commercial model for relying parties. Relying parties are charged a fixed fee when they initially register one of their customers for a GOV.UK Verify account, or when a customer with a pre-existing GOV.UK Verify account first uses that ID to transact with the relying party. This model allows the Cabinet Office to recoup the IDP charge over time without loading the full cost on the first relying party to register a customer for a GOV.UK Verify identity.

The development of ubiquitous digital identity that meets agreed standards and can be used across public and private sector, will lead to a range of commercial models. For example, a much lower "per-authentication" charge might be offered in place of the existing, relatively high "per-registration/first use" charge. Consortia of hub providers and IDPs could choose to commoditise identity on the basis that real value lies in additional attributes, delivered through the attribute exchange ecosystem. It is much easier for a relying party to calculate return on investment for attribute provision than it is for identity on its own.

It is important that this commercial diversity is allowed to develop, as different market sectors are likely to benefit from different commercial models, and competition will drive down prices. It is equally important that local authorities are able to choose from these private sector models should they wish to.

Enabling this evolution would stimulate the market for federated identity and achieve the volumes necessary to allow the market to thrive. There are wider economic benefits to be derived from allowing GOV.UK Verify to achieve its full potential. We have modelled these for local government in the logic chain below, but the same principles apply to the central government and the private sector.

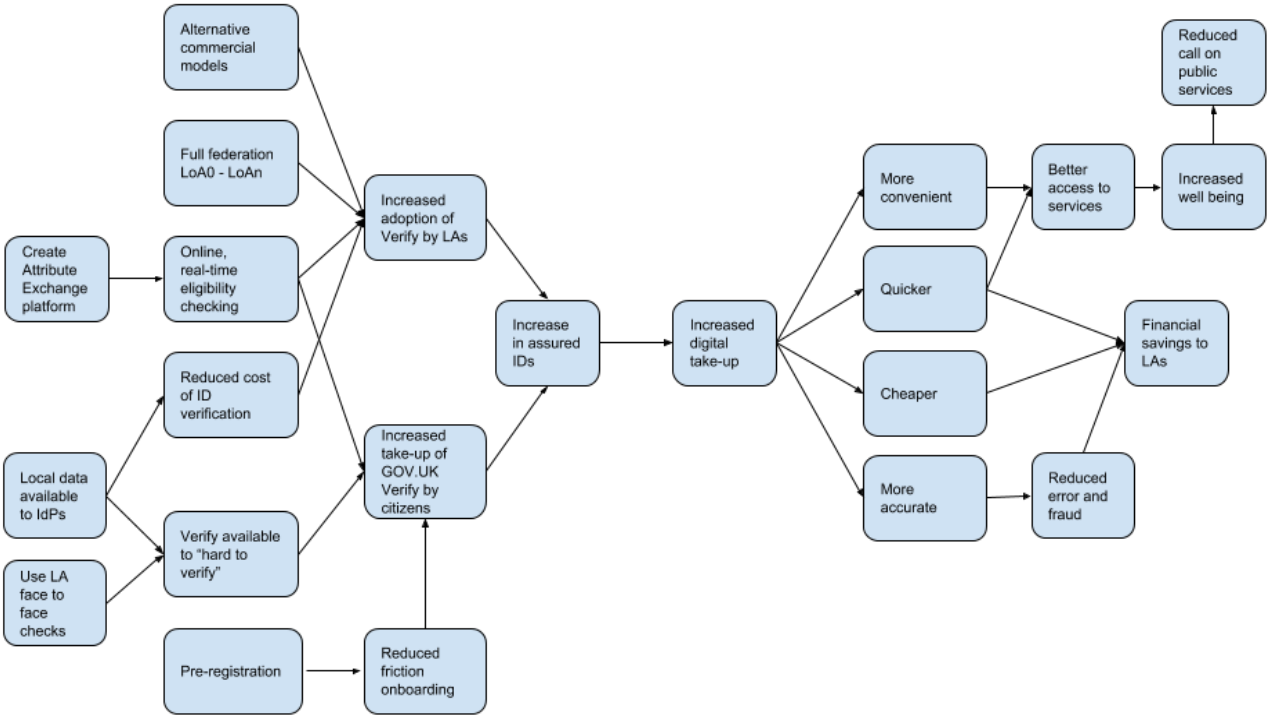


Diagram 6. Logic chain of economic benefits

CONCLUSIONS AND RECOMMENDATIONS

This project has demonstrated that local authorities collect and manage data that would have high value in the GOV.UK Verify identity proofing and verification process, particularly for thin-file customers who would not otherwise pass the GOV.UK Verify registration process.

The business case demonstrates that local authorities could derive substantial value from implementing GOV.UK Verify and an associated attribute exchange ecosystem, and that IDPs would also benefit from using data collected by LAs, and opening up the LA market for identity services.

We have modelled a workable technical solution to making local data available to GOV.UK Verify identity providers, and started the process of designing a user interface that could successfully weave together local authority transactions with a streamlined GOV.UK Verify registration process.

We have developed, validated and communicated our findings through a series of industry consultation events.

Project recommendations are that:

A. a Beta project is conducted to test and develop the outputs from the Alpha project with a wider range of local authorities and local authority customers;
B. the Beta project is used to:
    - implement a live technical infrastructure based on the model developed in Alpha;
    - demonstrate, in practice, the use of local authority data to help the hard to verify register for a GOV.UK Verify account to LOAn, with the user's consent;
    - demonstrate trust elevation over time, from simple logins to LOA2, using data collected in the DLB;
    - demonstrate the viability of self-certification of local data sources;
    - carry out user experience research to validate and develop the user interface outputs from the Alpha project;
    - test the enhanced functionality for GOV.UK Verify recommended in this document;
    - work with DWP to demonstrate how active local authority involvement in identity proofing and verification would deliver benefits in the Universal Credit application process.

APPENDIX A - PROJECT PARTICIPANTS

Digidentity	GOV.UK Verify Identity Provider Involved in technical design and technical integration
Etive	Project sponsor and supplier of the Digital Log Book (DLB). Involved in technical design, technical integration, user interface design, and industry consultation.
Pete Gale, ID Research	Advice on lessons learnt from GOV.UK Verify
GB Group	GOV.UK Verify Identity Provider. Involved in technical design, information governance, and user interface design
Government Digital Service	Project assurance
Greater London Authority	Involved in business case development
Ian Imeson Consulting Ltd	Involved in technical design, technical integration, information governance, user interface design and industry consultation
Ian Litton, Positive Attributes Ltd	Project coordinator. Involved in technical design, technical integration, information governance, user interface design, industry consultation and authoring project blogs and papers.
London Borough of Hackney	Relying party. Involved in information

	governance and business case development
London Borough of Tower Hamlets	Relying party. Involved in information governance and business case development
Mvine	Hub provider. Involved in technical design, technical integration, and user interface design.
Post Office	GOV.UK Verify Identity Provider. Involved in technical design, technical integration, information governance, and user interface design
techUK	Involved in organising, coordinating, and hosting industry consultation events.

APPENDIX B - INITIAL USER INTERFACE DESIGNS

As part of the project we have developed an example set of screens to illustrate how the user journey for thin-file customers could be simplified. Key features of the customer journey are:

1. upfront communication with users about the journey they are embarking on, and how GOV.UK Verify will figure in that journey. Some testing of this approach has already been done in the context of the Warwickshire County Council Blue Badge private beta project[15]. It is also a common service pattern for the Etive Digital Log Book, with users typically having a face to face interview as part of the social housing process, during which the Digital Log Book is introduced;

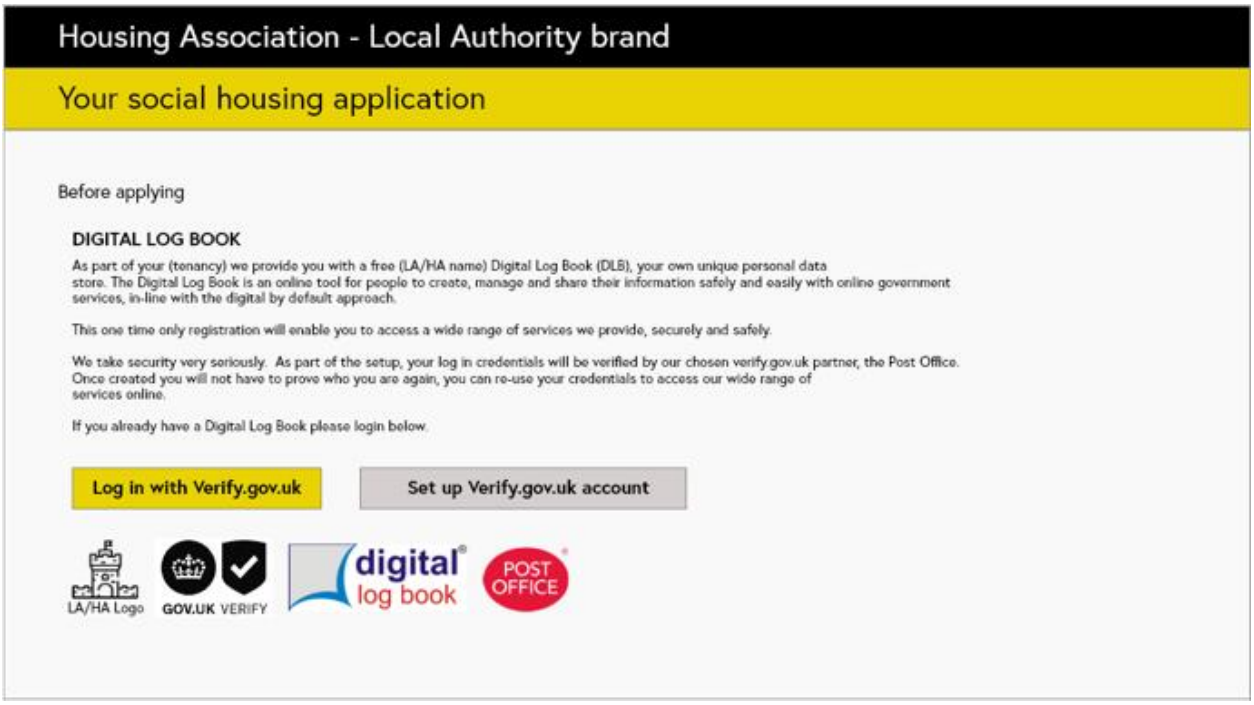
[15] For more information on this private beta project see https://dwpdigital.blog.gov.uk/2017/09/19/helping-citizens-choose-how-their-data-can-work-for-them/

2. use of a single IDP rather than offering the user a choice of IDPs. This reduces the conceptual complexity of Verify for its users. User choice can still prevail in this environment. A user could use a pre-existing digital ID from a different certified IDP with the relying party, and they could still register with more than one certified IDP in different contexts and use different accounts with different relying parties. We believe this would maintain the Privacy and Consumer Advisory Group (PCAG) requirement for multiplicity[16];
3. creation of a simple login account with the IDP. Our user journey starts with the creation of a simple login account by the IDP. The user is able to create a secure account, protected by two-factor authentication, with the minimum amount of friction, so they can get on with the job in hand;
4. use of locally sourced data. Once the user has completed the job in hand, the transaction information that has been entered and validated by the local authority can be passed to the IDP, with the user's consent, to elevate the level of assurance associated with their account.

EXAMPLE SCREENS

The journey would start with an explanatory email (not shown here), explaining the role of the Digital Log Book in the social housing application, and the use of GOV.UK Verify for identity proofing and verification. The email would contain a link to set up a Digital Log Book (or log in, if the user already has one). This would link to the screen below.

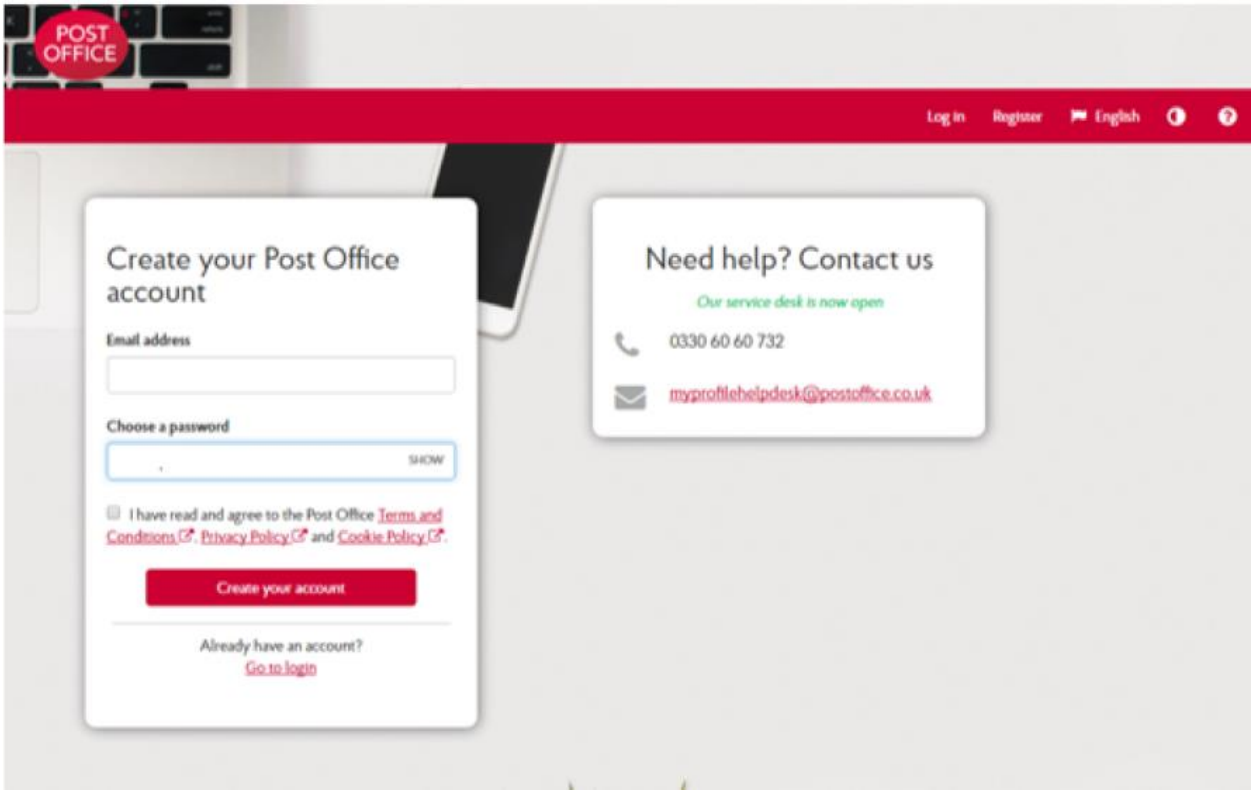
[16] See https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles

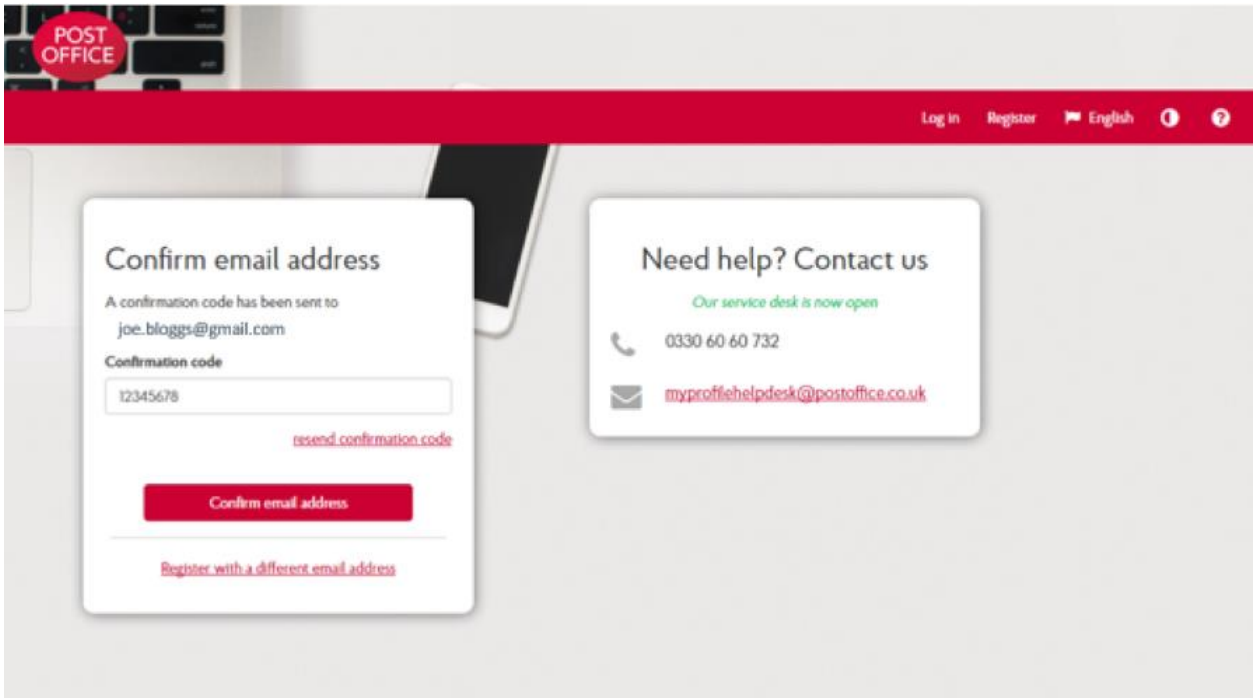


We will follow the route taken by a user who is setting up a new digital log book.

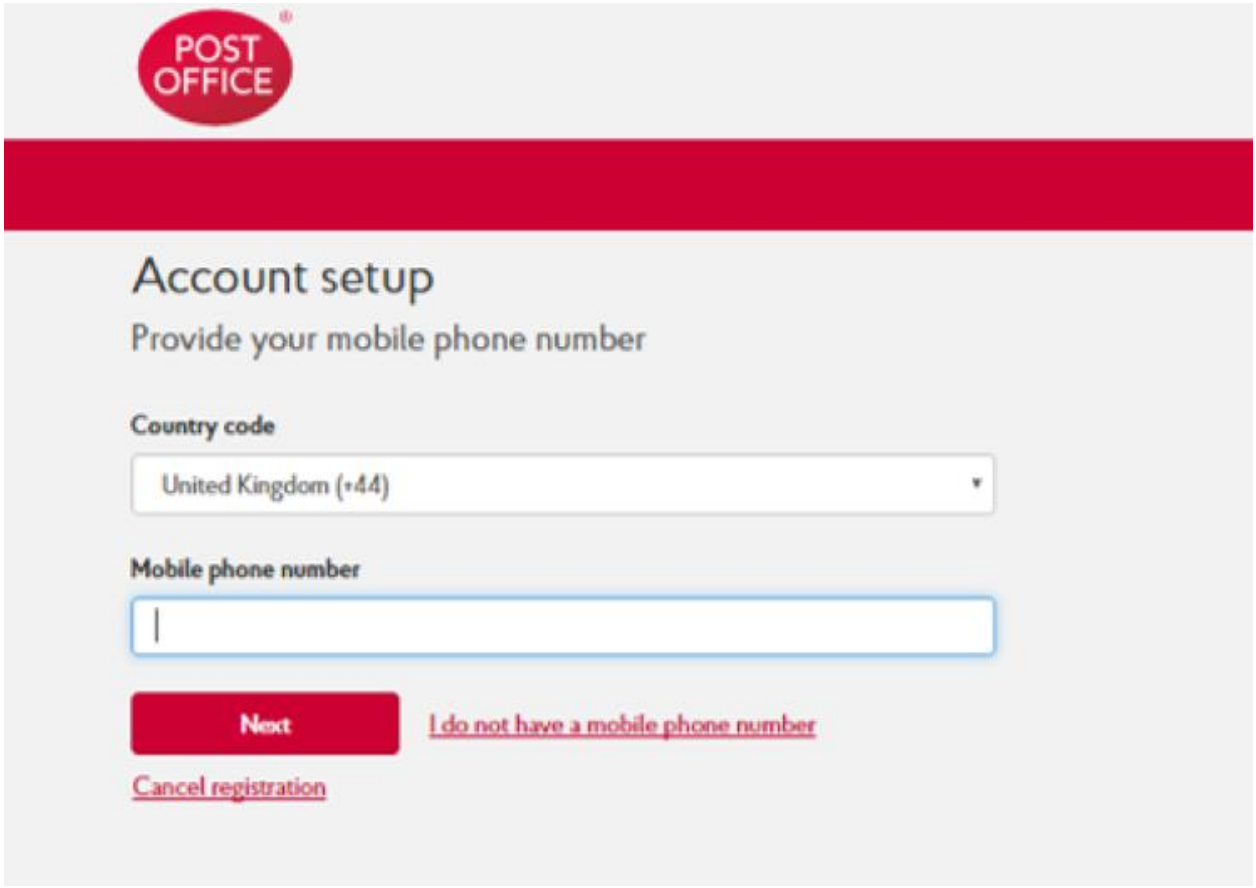
The first step is for the user to set up a simple login. This can be done with minimum friction, allowing the user to get on with the job of completing their social housing application. The pre-registration approach modelled here does not give the user a choice of IDP, but directs them straight to the relying party's chosen IDP, the Post Office in this case. This is designed to further reduce friction, and remove some of the cognitive dissonance associated with the concept of federated identity.

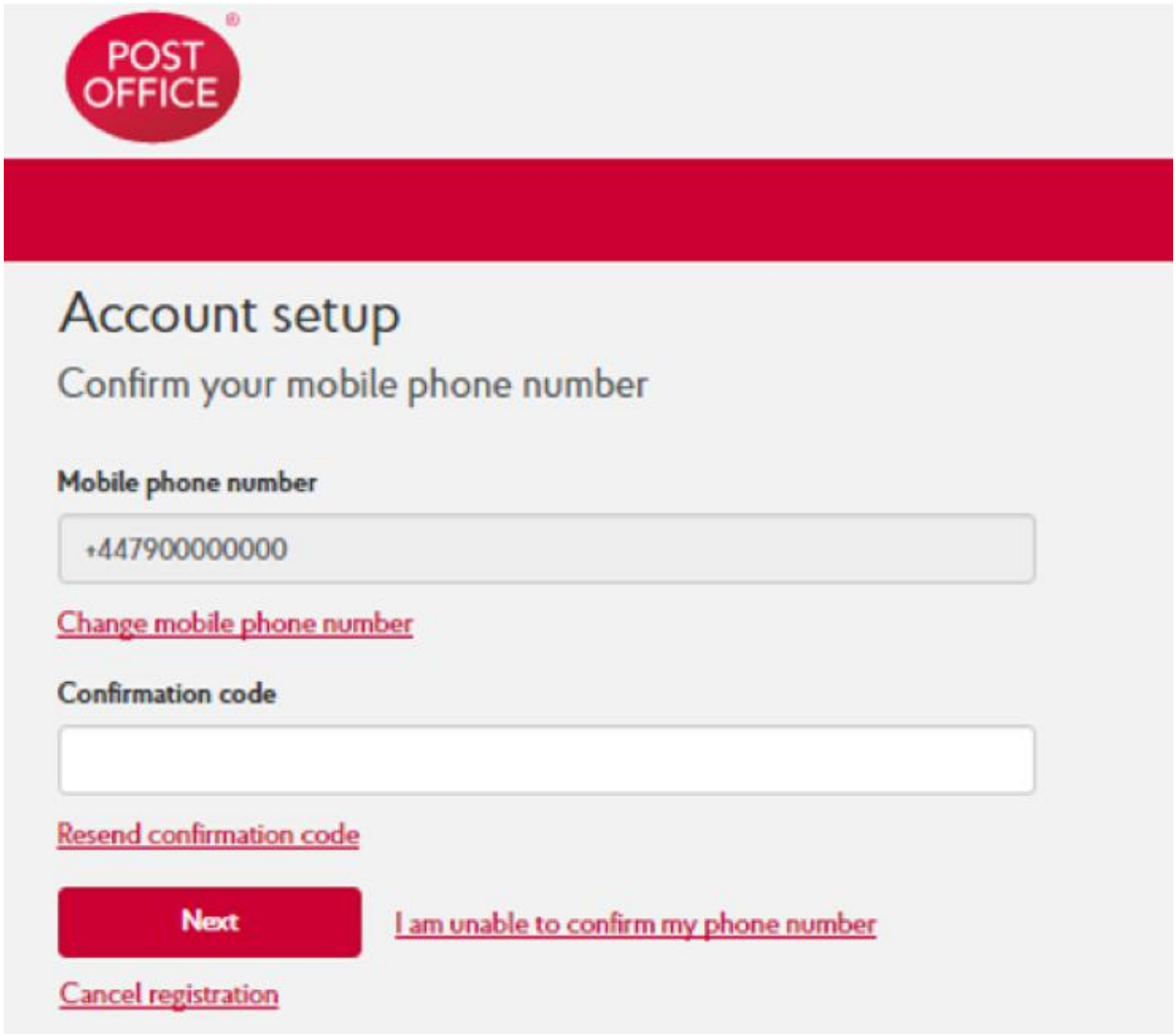
User experience research will be needed to test how well this approach works, and to identify how to handle branding around GOV.UK Verify and the IDP.

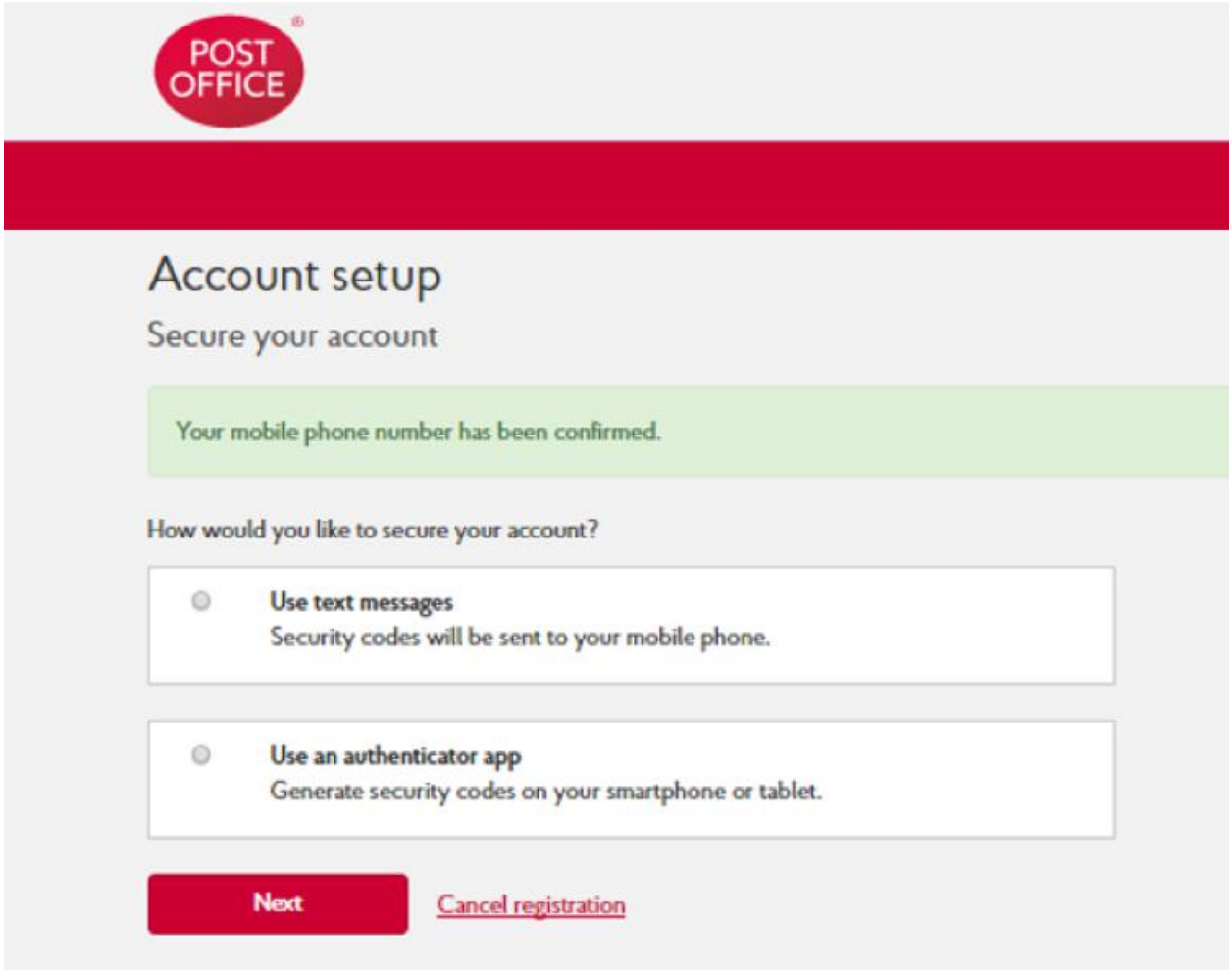

POST OFFICE
Log in
Register
English
Create your Post Office account
Email address
Choose a password
SHOW
I have read and agree to the Post Office Terms and Conditions, Privacy Policy and Cookie Policy.
Create your account
Already have an account?
Go to login
Need help? Contact us
Our service desk is now open
0330 60 60 732
myprofilehelpdesk@postoffice.co.uk


POST OFFICE
Log in
Register
English
Confirm email address
A confirmation code has been sent to
joe.bloggs@gmail.com
Confirmation code
12345678
resend confirmation code
Confirm email address
Register with a different email address
Need help? Contact us
Our service desk is now open
0330 60 60 732
myprofilehelpdesk@postoffice.co.uk

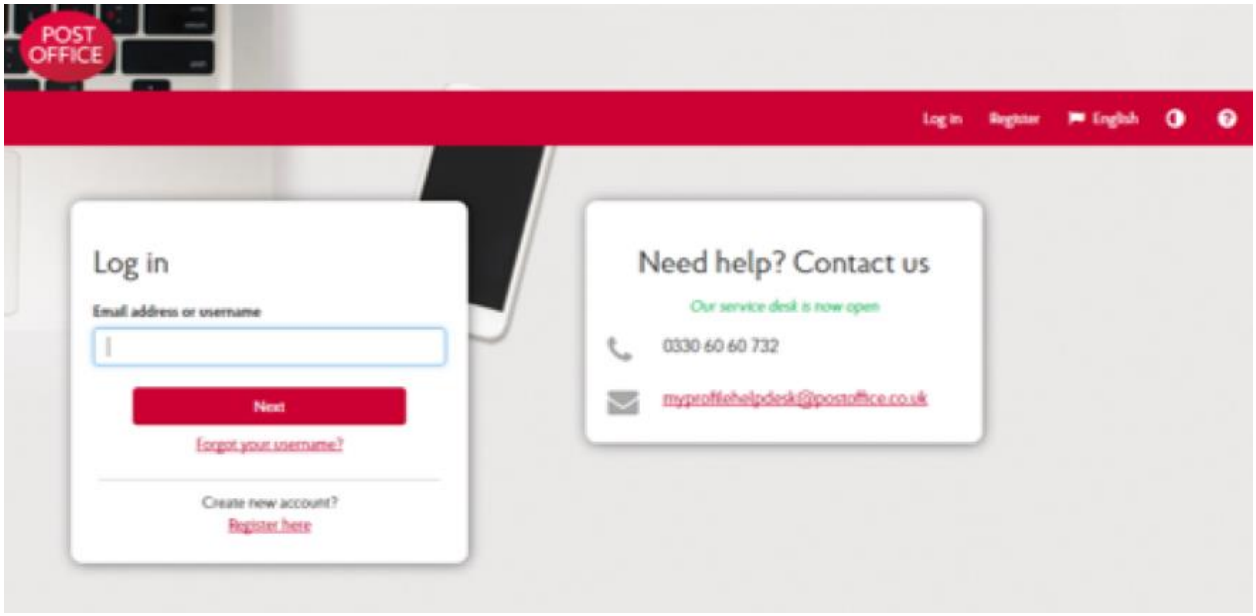
Two factor authentication reduces the possibility of another user hijacking a simple login, an important consideration given that the user will be given the option to elevate the level of assurance associate with their ID at a later date.

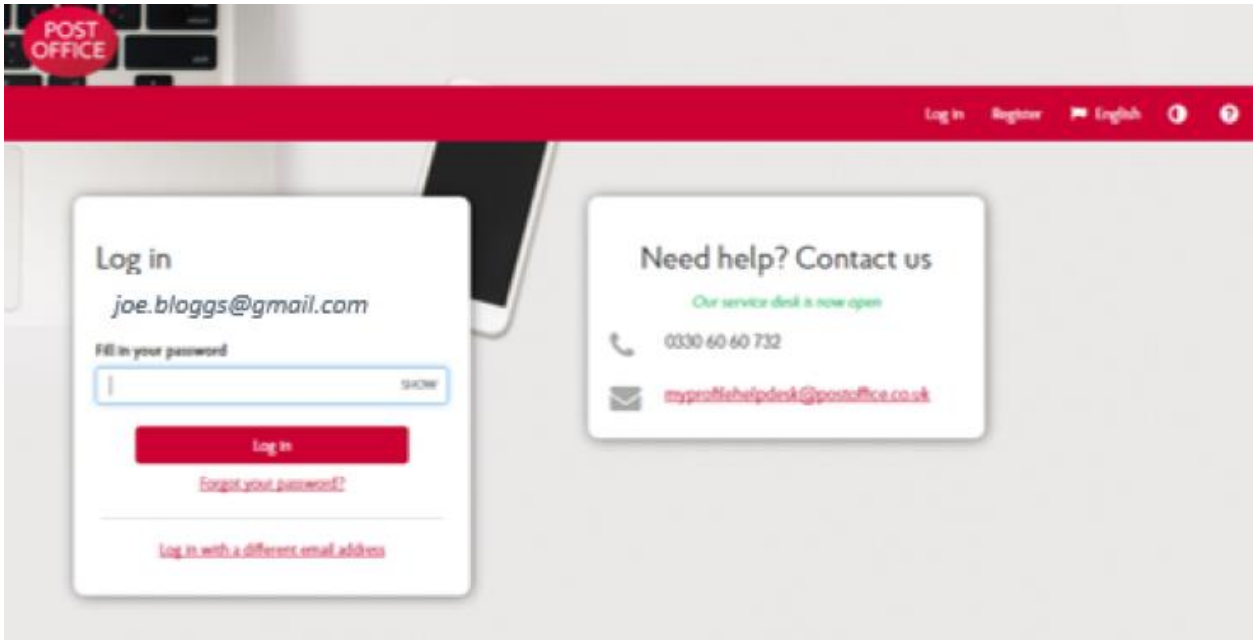



POST OFFICE
Account setup
Confirm your mobile phone number
Mobile phone number
+447900000000
Change mobile phone number
Confirmation code
Resend confirmation code
Next
I am unable to confirm my phone number
Cancel registration

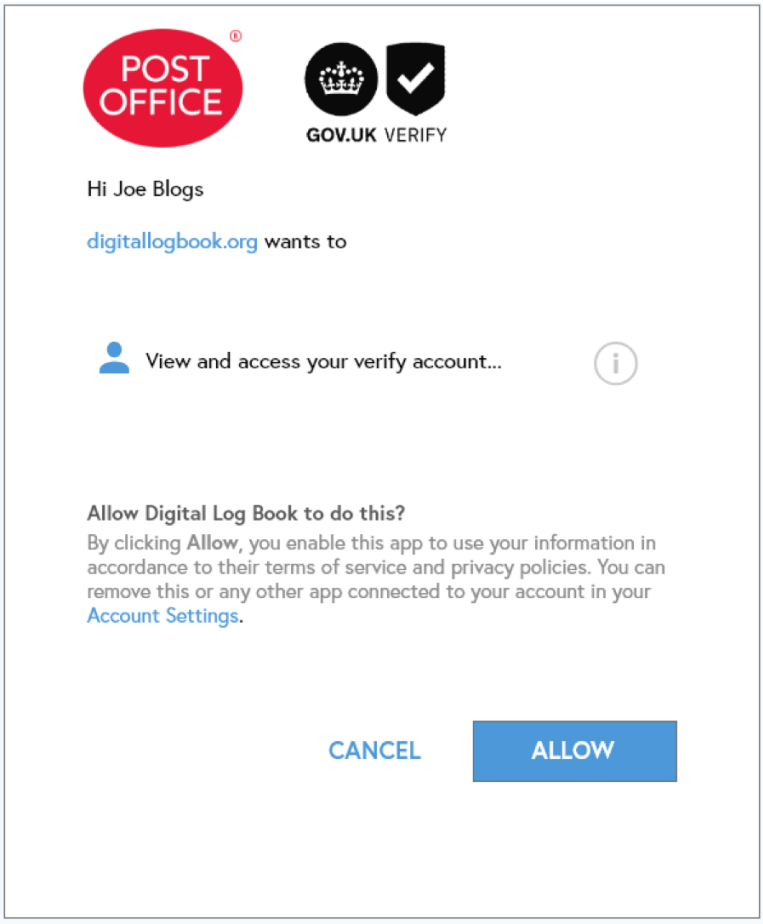


The user can now log in with their new simple login. They will receive the second factor challenge in the process (not shown).


POST OFFICE
Log in
Register
English
Log in
Email address or username
Next
Forgot your username?
Create new account?
Register here
Need help? Contact us
Our service desk is now open
0330 60 60 732
myprofilehelpdesk@postoffice.co.uk

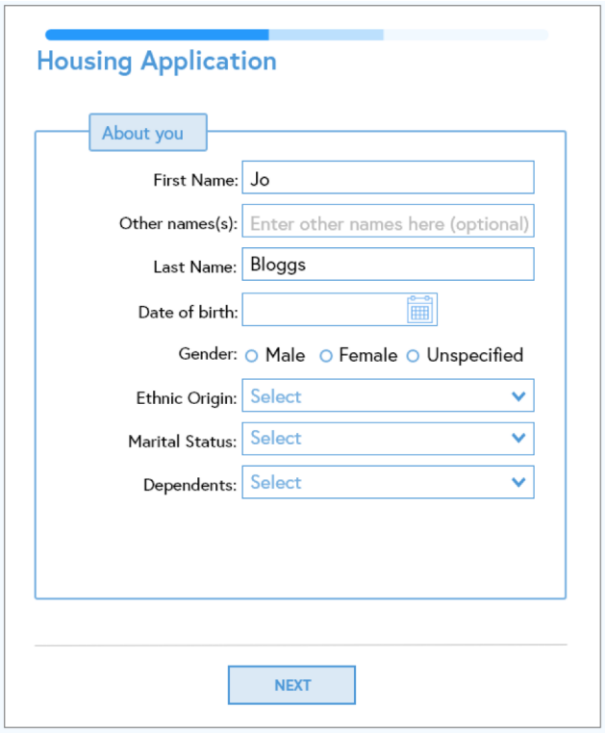

POST OFFICE
Log in
Register
English
Log in
joe.bloggs@gmail.com
Fill in your password
SHOW
Log in
Forgot your password?
Log in with a different email address
Need help? Contact us
Our service desk is now open
0330 60 60 732
myprofilehelpdesk@postoffice.co.uk

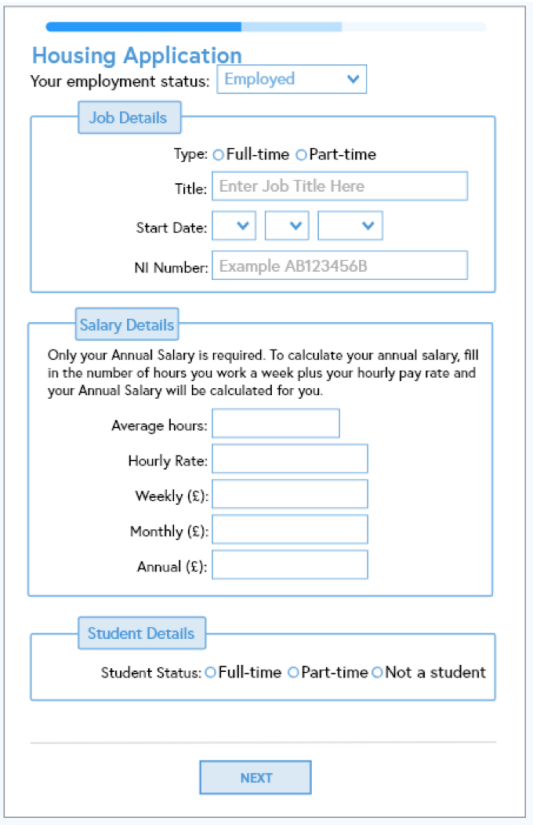
The user is shown a typical dialogue for when a federated identity is being used to access a particular application (the Digital Log Book in this case).

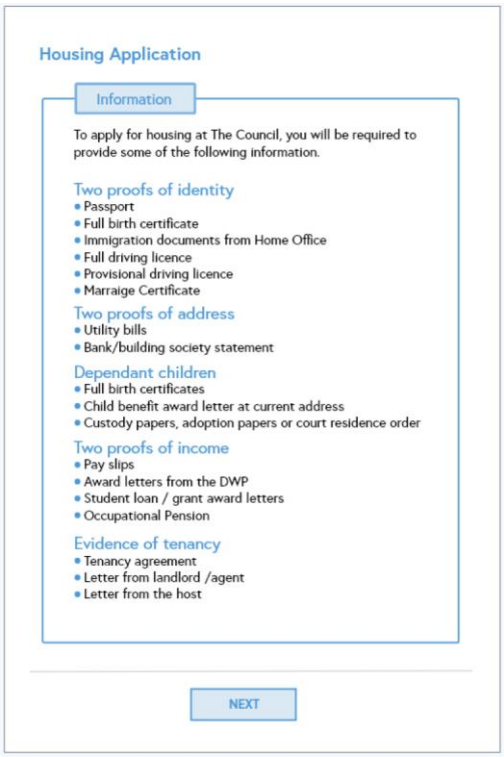


As part of the set-up process of the Digital Log Book, the user is asked to sign up to the conditions of use and the privacy policy.

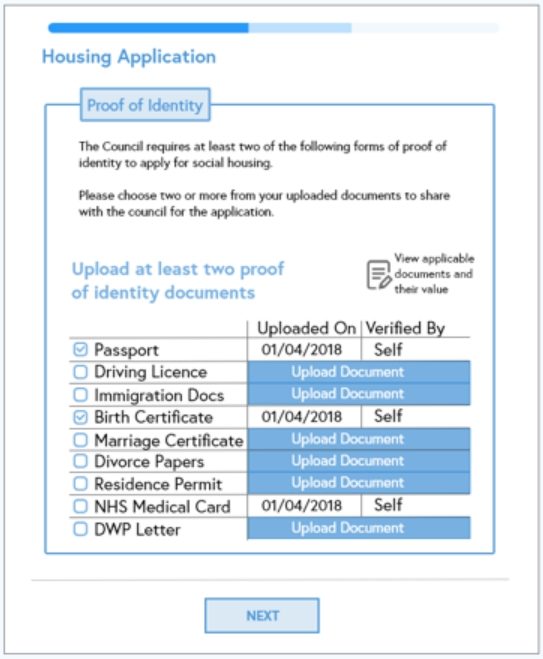
The user can now start their social housing application. In the process they will self-assert a lot of information, and upload a series of documents, that will later be used to help them elevate the level of assurance associated with their Post Office GOV.UK Verify account. All of the information on the following screens is required to assess if the applicant is eligible to be added to the social housing register.

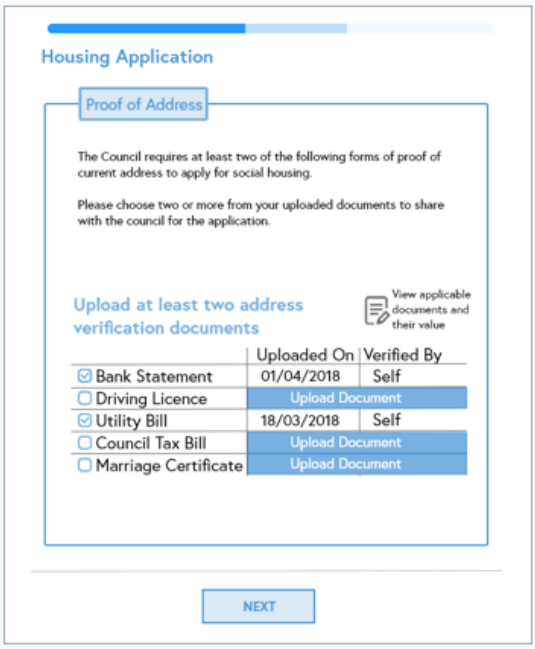


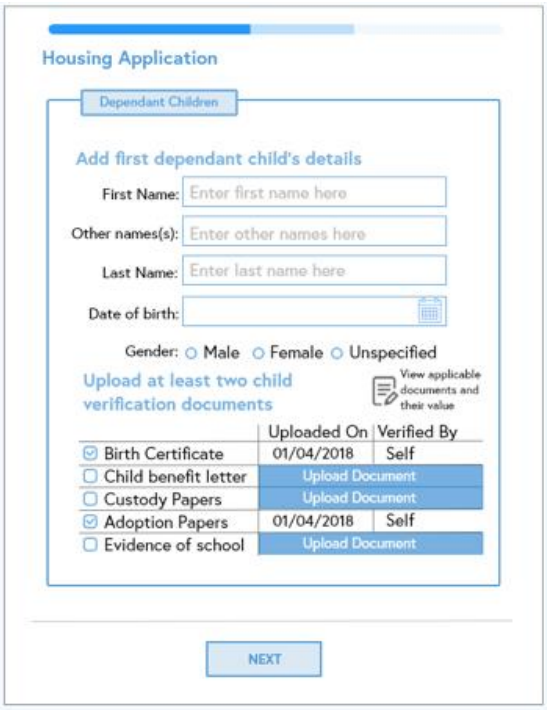

Housing Application
Your employment status: Employed
Job Details
Type: Full-time Part-time
Title: Enter Job Title Here
Start Date:
NI Number: Example AB123456B
Salary Details
Only your Annual Salary is required. To calculate your annual salary, fill in the number of hours you work a week plus your hourly pay rate and your Annual Salary will be calculated for you.
Average hours:
Hourly Rate:
Weekly (£):
Monthly (£):
Annual (£):
Student Details
Student Status: Full-time Part-time Not a student
NEXT


Housing Application
Information
To apply for housing at The Council, you will be required to provide some of the following information.
Two proofs of identity
Passport
Full birth certificate
Immigration documents from Home Office
Full driving licence
Provisional driving licence
Marraige Certificate
Two proofs of address
Utility bills
Bank/building society statement
Dependant children
Full birth certificates
Child benefit award letter at current address
Custody papers, adoption papers or court residence order
Two proofs of income
Pay slips
Award letters from the DWP
Student loan / grant award letters
Occupational Pension
Evidence of tenancy
Tenancy agreement
Letter from landlord /agent
Letter from the host
NEXT

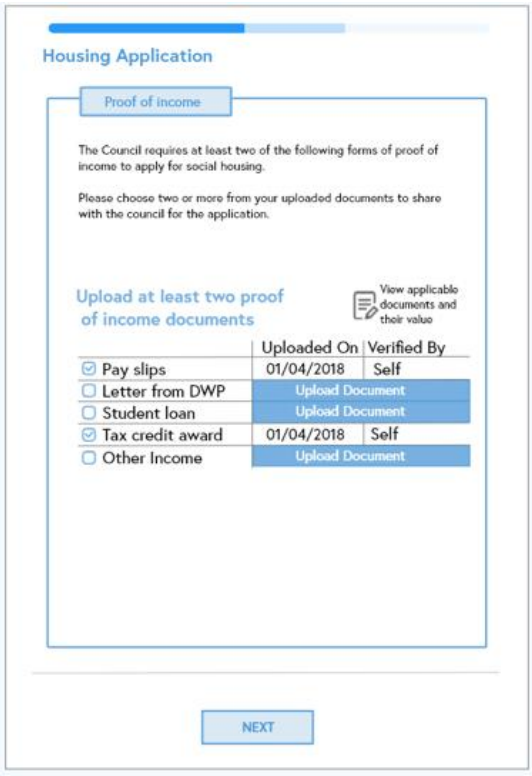
Documents can be uploaded and stored in the DLB.






Housing Application
Dependant Children
Add first dependant child's details
First Name: Enter first name here
Other names(s): Enter other names here
Last Name: Enter last name here
Date of birth:
Gender: Male Female Unspecified
Upload at least two child verification documents
View applicable documents and their value
Uploaded On
Verified By
Birth Certificate 01/04/2018 Self
Child benefit letter Upload Document
Custody Papers Upload Document
Adoption Papers 01/04/2018 Self
Evidence of school Upload Document
NEXT


Housing Application
Dependant Children
Add second dependant child's details
First Name: Enter first name here
Other names(s): Enter other names here
Last Name: Enter last name here
Date of birth:
Gender: Male Female Unspecified
Upload at least two child verification documents
View applicable documents and their value
Uploaded On
Verified By
Birth Certificate 01/04/2018 Self
Child benefit letter 01/04/2018 Self
Custody Papers Upload Document
Adoption Papers Upload Document
Evidence of school Upload Document
NEXT



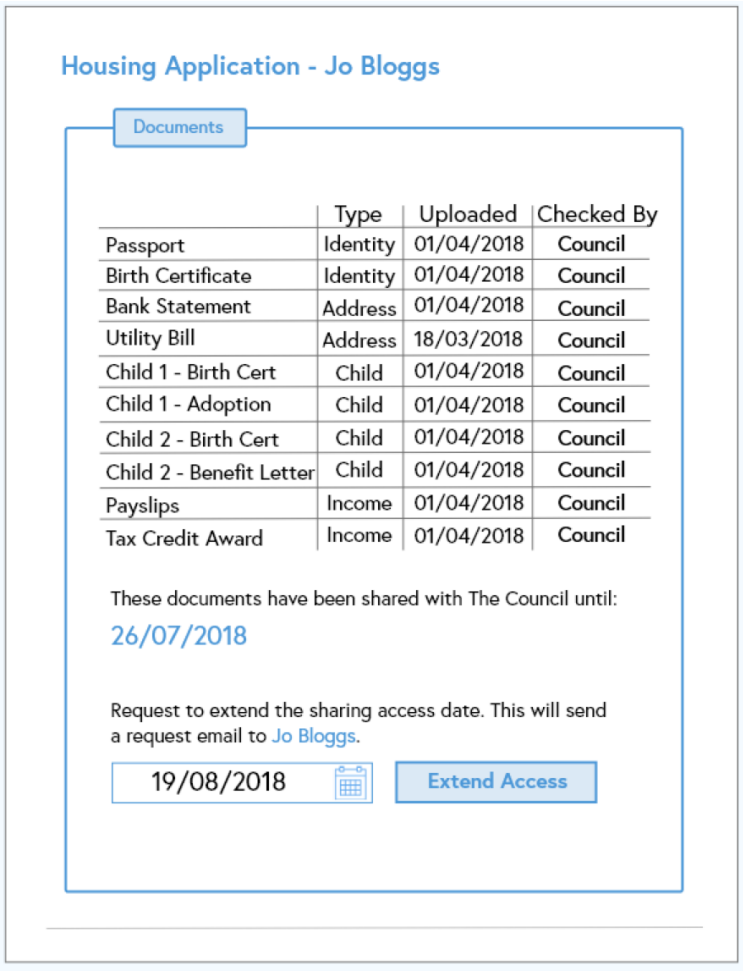
The user is given a summary of the documents uploaded, and is able to share these with the council for a set period of time. They can choose not to do this, and to share the original documents, but current usage of the Digital Log Book indicates that most users will share electronically as it is more convenient and speeds up the application process.

If the applicant meets the eligibility requirements, the councils we have worked with require them to attend a face to face interview so that original documents can be

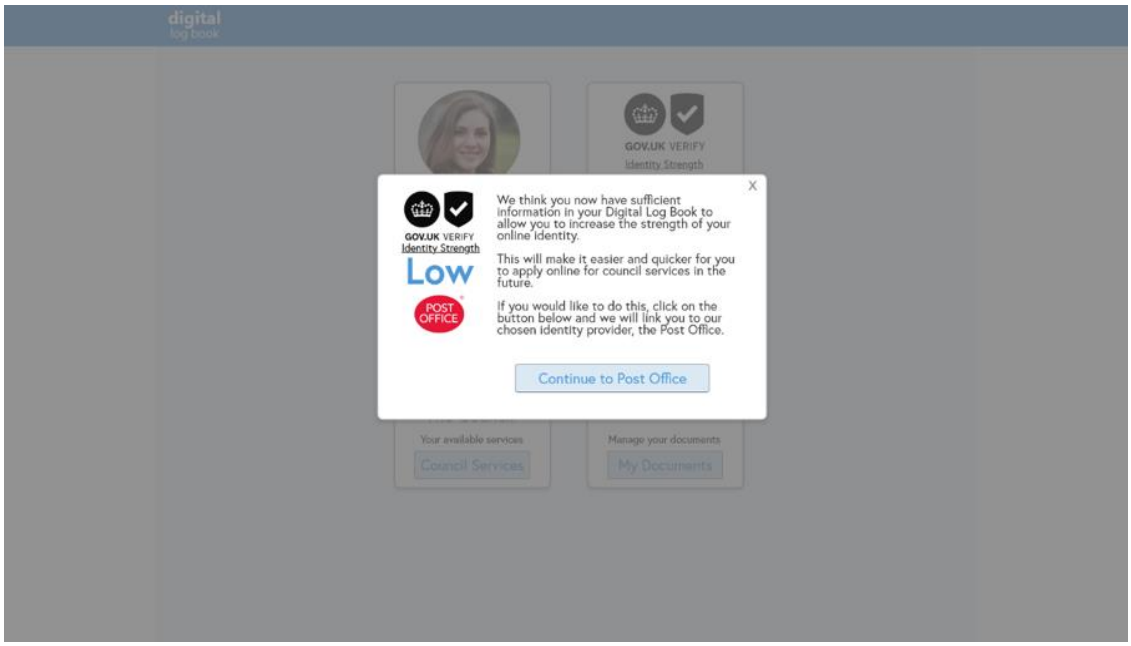
checked, and a photograph of the applicant can be taken and added to the case file. This is important to ensure that the person who later comes to view a property is the same person who originally applied.

The case worker would log on to the Digital Log Book, view the records already shared by the DLB user, and confirm that they have checked the original documents. They would also record if, for example, they had used approved scanning solutions to check for fraudulent documents. This would increase the value of the data to the IDPs. Face to face checks could potentially support LOA3 identities.

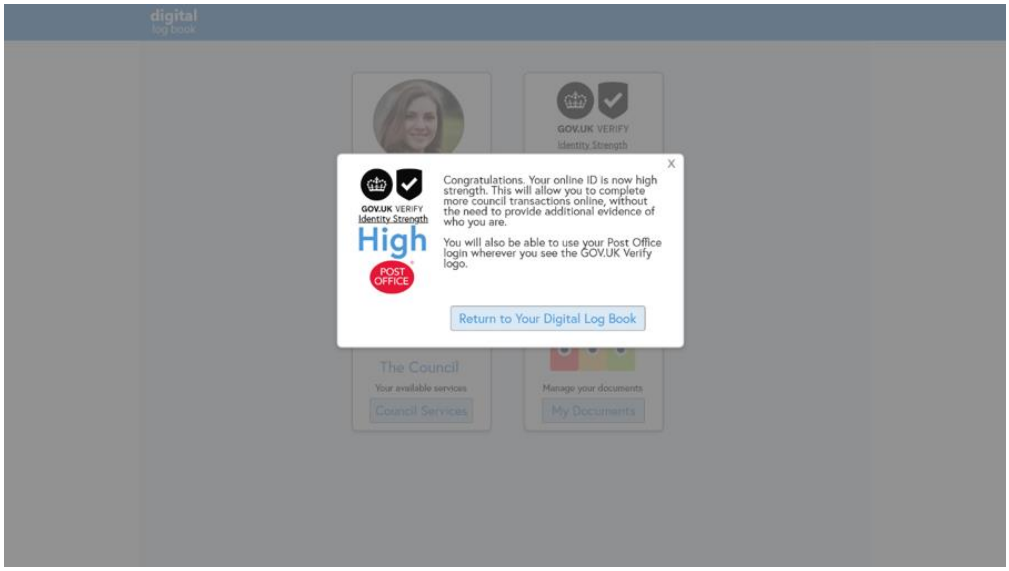
The council could request an extension to the sharing access date if required.



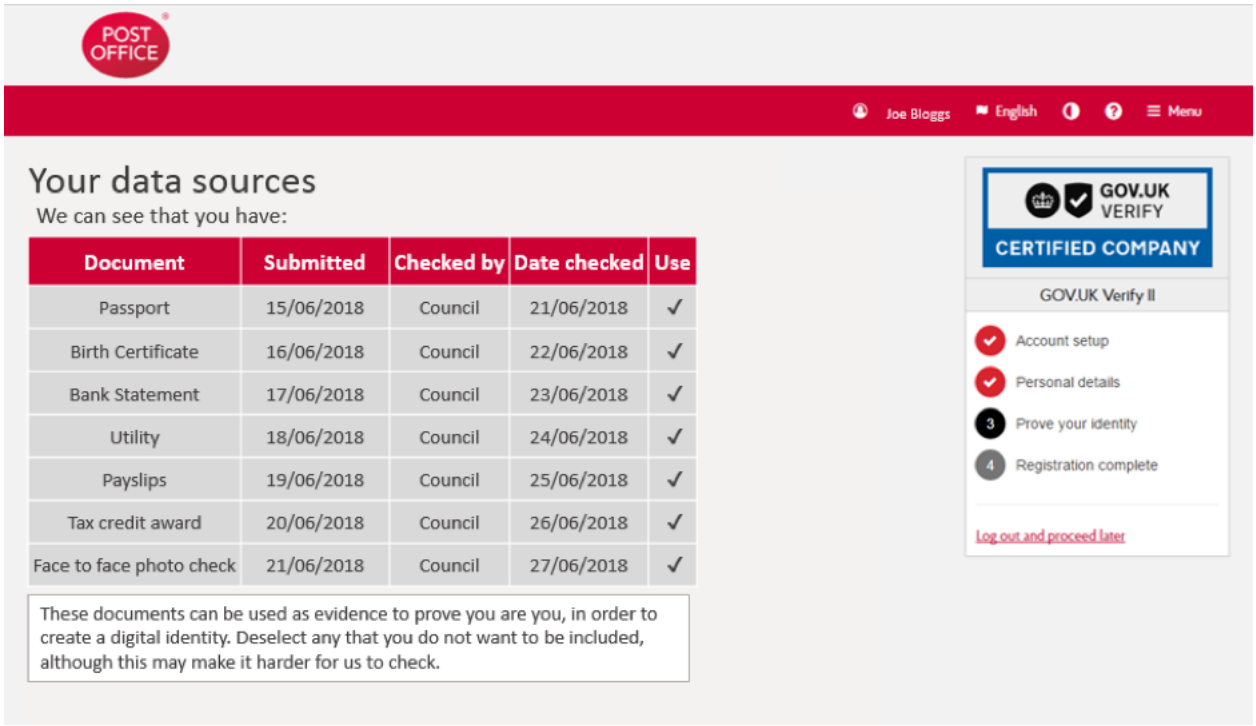
When the user next logs on to their DLB they will be offered the opportunity to increase the strength of their GOV.UK Verify account. The dialogue below shows the user that their account is currently low strength (i.e. a simple login). The incentive for increasing the strength of their account is access to a wider range of online services.



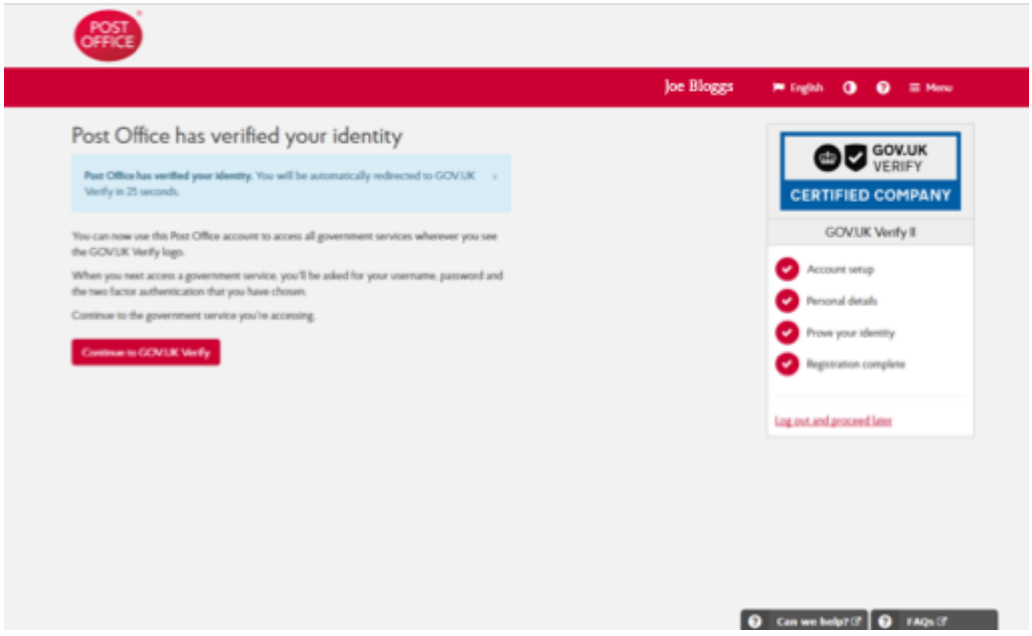
The user is redirected to the Post Office. In the background the Post Office will receive a SAML message containing the relevant data from the DLB, plus associated metadata. This can be combined with the IDP's normal sources of data in an attempt to bring the user's account up to LOA1 or LOA2.



One option is for the IDP to redisplay the data sources that are being shared from the DLB and to give the user the choice at that point of deciding if they want to share the relevant documents with the IDP



The IDP would confirm the success of the trust elevation before handing back to the DLB:



APPENDIX C - DRAFT TECHNICAL DESIGN

HIGH LEVEL ARCHITECTURE

The overall architecture is represented in the following diagram:

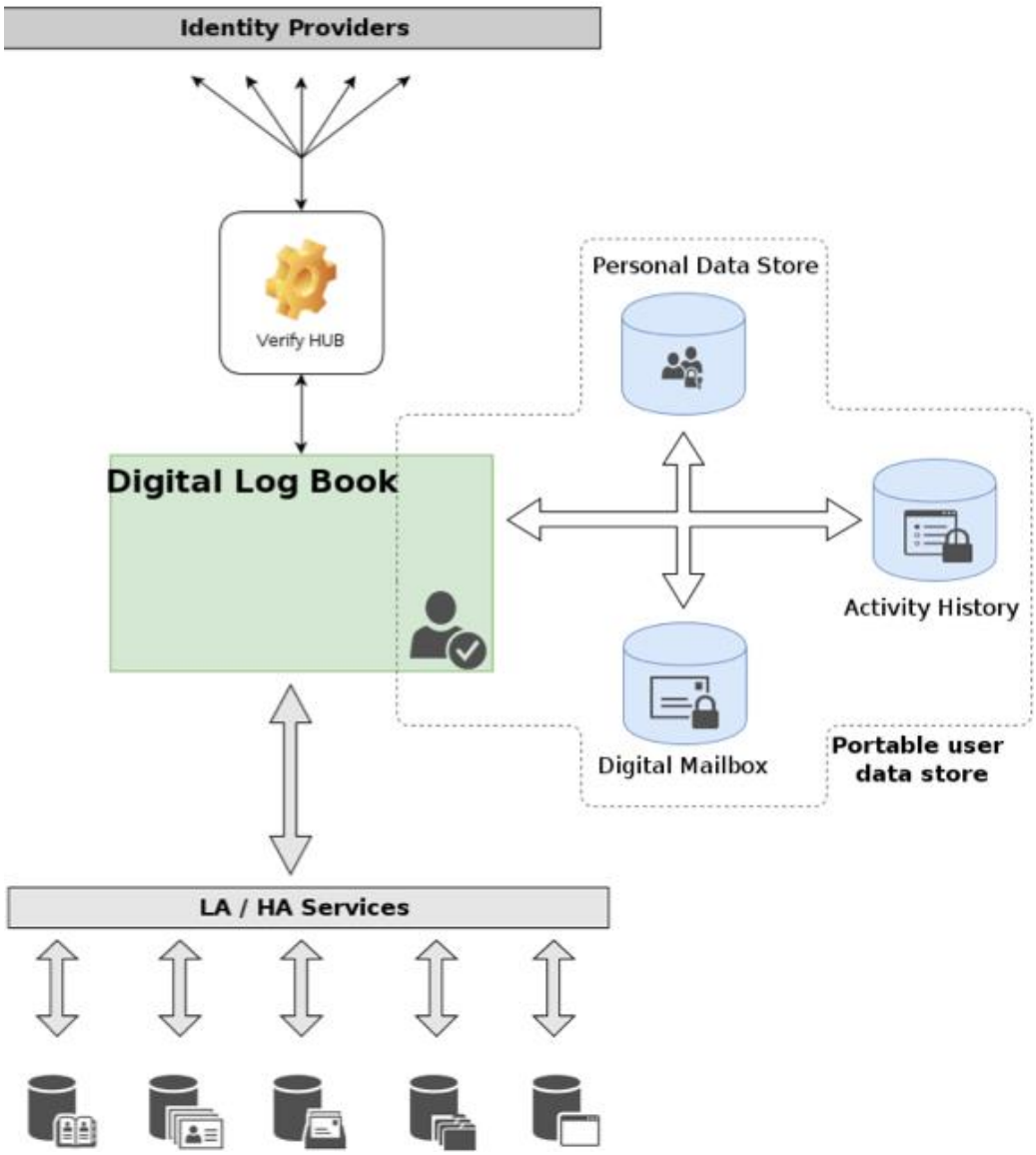


Diagram 1. High level architecture

The Digital Log Book sits in front of a council's back office systems and presents a single integration point to the GOV.UK Verify hub. The links between the back- office systems and the Digital Log Book can be implemented in a number of different ways, depending on the council's preferences and the capabilities of their back- office systems.

A metadata schema would describe the local data in a way that would allow the IDPs to quantify its value in the identity proofing and verification process. The example schema below includes data items relating to social housing transactions, but the schema could be extended to cover different transactions and other sources of data.

Meta-data	Data category (ID, Activity History, KBV)	Date data recorded	Self-asserted or verified?	Method of validation	Mandatory or Optional	Activity History definition	User's level of assurance when data was recorded (LoAx)	Currency (last updated)	Cross-checked against...
data items									
forename	ID								
surname	ID								
middle name	ID								
dob	ID								
passport no	ID								
passport name (first name, middle name, last name)	ID								
passport expiry	ID								
driving licence name (first name, middle name, last name)	ID								
driving licence address	ID								
driving licence number	ID								
Housing repair request	AH								
Anti-social behaviour report	AH								
Housing bid	AH								
House viewing	AH								
Monthly rent	KBV								
Tenancy start date	KBV								
DWP Benefit Amount									
etc									
Current LoA									
IdP PID									

Diagram 2. Metadata scheme

The metadata items are described in more detail in the following table.

Data item	The data being presented
Data category (ID, Activity History, Knowledge Based Verification)	Describes the type of data represented and which Identity Verification category it sits within.
Date data recorded	The date when the data item was first recorded
Currency (last updated)	The date when the data item was last updated

Self-asserted or verified?	Has the data been verified by a council officer
Method of verification	E.g scanning technology used, manual check. We need to develop a pick list for this item.
Mandatory or Optional	Will this data item always be present, or only sometimes?
Activity History definition	Is the activity history in question of high, medium or low value. This will be based on an agreed categorisation. For example, a history of automated payments would be of low value.
User's level of assurance when data was recorded (LoAx)	This will indicate if the data (particularly if self-asserted) was bound to a more or less highly assured identity
Cross-checked against...	Has this data item been crossed checked in any way? E.g. has the amount on an award notice from the DWP been cross-checked against payments in to the individual's bank account?

Table 3. Description of metadata items.

The existing GOV.UK Verify SAML profile would be extended to present the DLB data to the IDPs via a hub. The following schematic maps the SAML calls in the customer journey:

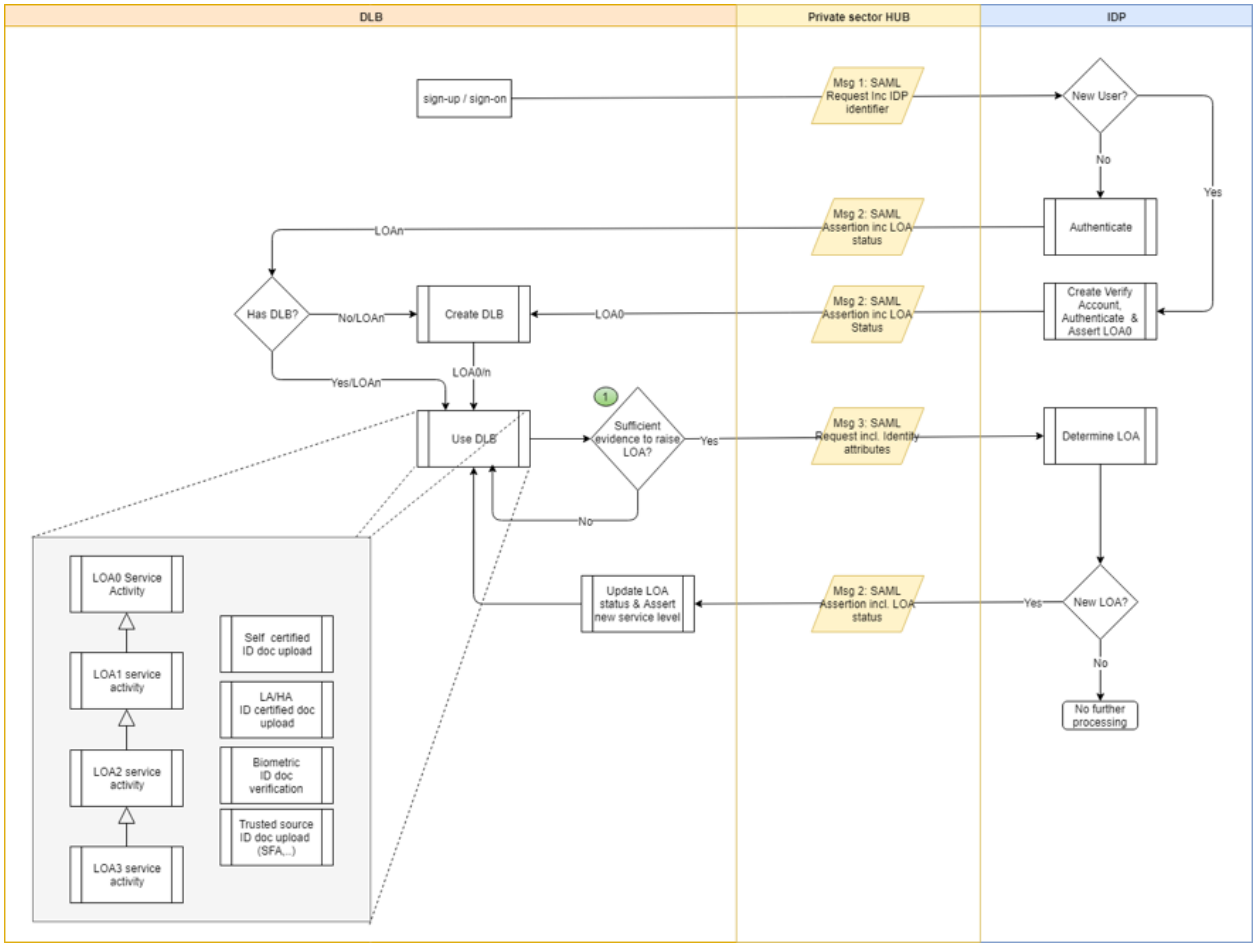


Diagram 3. Schematic of SAML calls

In the proposed model it is possible for a user, over time, to elevate the level of assurance (LOA) associated with their GOV.UK Verify account as they assemble more identity-related data in their DLB. They could progress from a simple login, to LOA1 and then LOA2.

APPENDIX D - ORGANISATIONS ATTENDING CONSULTATION EVENTS[17]

ACAMS	GoodPeople	Person Centred Software
Agilisys	GOSS	Post Office
Ian Imeson Consulting Ltd	London Borough of Hackney Council	Royal Borough of Kensington & Chelsea
Barclays	Housing Associations Charitable Trust	Rory MacDonald
Barking & Dagenham	Idemia	Sitekit
Capita	IEG4	London Borough of Sutton Council
Civica	iStandUK	Tata Consultancy Services
Consult Hyperion	Jadu	The Pirean Group of Companies
DWP	London Borough of Kingston	TISA
Etive	London Borough of Waltham Forest	London Borough of Tower Hamlets
Evernym	Local Government Association	Yoti
GBG	Mvine Limited	zInet
GDS	NHS Digital	
Greater London Authority	Northgate Public Services	

[17] Please note that attendance does not necessarily mean endorsement of views expressed in the paper

APPENDIX E - GLOSSARY OF TERMS

Attribute	A characteristic of a person or a thing
Attribute Exchange	A mechanism that allows a relying party to request information about a data subject from an attribute provider, online, and in real-time, with the data subject's explicit permission. The attribute exchange ecosystem is governed by a trust framework that covers technical, legal and commercial aspects of the ecosystem. Typically built using open standards protocols and specifications, such as oAuth2 and User Managed Access (UMA).
Attribute Provider	An organisation that can provide attributes about a person or a thing through the attribute exchange ecosystem
Federated Identity	A common set of policies, practices and protocols to manage identity and trust across organisations.
General Data Protection Regulation (GDPR)	A European regulation on data protection and privacy that replaced the 1995 Data Protection Directive (and the UK Data Protection Act 1998) on May 25th 2018.
Level of Assurance	The level of trust that can be put in a digital identity, based on the level of confidence that the person in possession of the digital identity is who they say they are. The UK government has defined the levels of assurance, and mapped them to

	international standards, in their Good Practice Guide 45[18]
Personal Data Store (PDS)	A secure data repository that is owned and managed by an individual user, even if it is initially issued to the individual by an organisation. The PDS provides the user with tools to control who they share their data with, in what circumstances, and for what purposes.
Relying Party	A service provider, organisation, or system that consumes and relies on the digital identities provided by an identity provider
Simple login	An unverified user account, set up to allow the user to authenticate, but without providing any proof of identity.

[18] https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual