Use Case #:

Create a legal Verify standard of identity for a thin file citizen.

Goal in Context:

To create an identity for a citizen applying for access to public services such as housing.

Preconditions:

The citizen understands what is happening as part of their application process, may or may not have forms of identification that meet GDS standards, such as a driving licence or passport but is willing and able to provide other forms of information for identification purposes.

Quite often the service provider will provide a list of accepted identity documentation, which might include a birth certificate, marriage/divorce papers, education certificates, bank statement, residence permit or NHS medical card.

Success Conditions:

A citizen provides a copy of original documents prescribed by the authority, first time. These documents will come from a prescribed list.

Frontline staff will be trained to check for document forgery, albeit at a low level.

Checked documentation is then uploaded into the citizen's DLB, time and date stamped and categorised. Once an agreed threshold of documents has been achieved automatically sent to an IDP (identity provider) in order to confirm Level of Assurance (LoA).

A legal standard of identity is created for the citizen.

If not a high enough standard to access high value services, then over time their level of assurance can be elevated with the use of activity history, other forms of identity and/or knowledge based verification (KBV).

If supporting a homeless person for example, where no identification exists, to create a low level of assurance for the person, so their levels of assurance can be elevated over time. This will bring the person into the eco-system enabling an identity to be established.

Failed Conditions:

There are arguably no failed conditions, as the objective is to create some form of digital identity for thin file citizen, focusing on the especially hard to reach who are in greatest need of support- such as homeless people.

With only 5 attributes:, given name, given date of birth, verified photograph, known gender and ethnicity, these attributes can be used to build the basic credentials of a person. Name and DoB may be wrong but can be changed/updated/reviewed.

Primary Actors:

Housing applicant, local authority, housing association or 3rd sector.

Secondary Actors:

Government department, such as DWP, service providers and support agency staff.

Triggers:

A thin file citizen will typically walk into a local hub (community facility run by a local authority for citizens to access support, information and advice) or they make visit local authority offices.

They will have to wait in a que in order to speak to a person to ask for advice related to their issue and what they need to do. In this instance a housing application.

Citizen will be directed towards an online portal in which they need to register and bid for a property. As part of the application process they will be required to provide some form of specified identity documentation.

If their bid application is successful the citizen will be invited in for an interview and may be asked to provide original copies of their submitted identity documents and a photograph of them may be taken. The housing officer, or person who takes the photograph, can confirm that the subject is the same as the photographs in provided id documents such as a passport. A quick and efficient visual confirmation.

Documentation will be checked for authenticity through a variety of means and other information such as income of benefits received against bank statements may be cross referenced.

Processes:

A personal data store, Digital log Book (DLB), will be created by/for the citizen as an aggregation point of information, owned and controlled by the citizen, ensuring GDPR compliance.

The DLB can be used for identity information, activity history and for future knowledge-based verification.

Basic set up data will include: Given name, address, phone number, NI number, DoB and gender and in some instances ethnicity.

Citizen, local authority, housing association etc can upload as much information about the citizen into their DLB. The citizen can upload a selfie by using their mobile phone and/or a third party can take and upload a verified photograph, which is then encrypted. A selfie, which has a certain value, can be replaced by a photograph taken by an authorised person, which will replace the selfie and be encrypted so it cannot be changed the latter has a higher value.

Other data will also be collected, typically from the local authority who might already hold data on the citizen. Data can also then be pulled in from a variety of other trusted sources of data. Data can be verified by being crossed referenced with other data sources, in time through an ‘attribute exchange’.

This information is then collected and stored in the citizens personal data store and this information can then be used to create an identity account to Verify standards for thin file citizens. This will allow the citizen to complete an online transaction, in this case a housing application. LA data, and other sources of data, will be sufficient to supplement the data already available to identity providers (IDPs) for thin file citizens to achieve a high level of assurance. The DLB personal data store will provide a suitable aggregation point for that data, under the user’s direct control and consent.

1. Demonstrate, in practice, the use of local authority data, aggregated in the DLB, to help the hard to verify register for an LoA1 or LoA2 account to GOV.UK Verify standards, with the user’s consent.

2. Demonstrate trust elevation over time, from a self-asserted entry level account to LoA2, using data collected in the DLB.

Workflow:

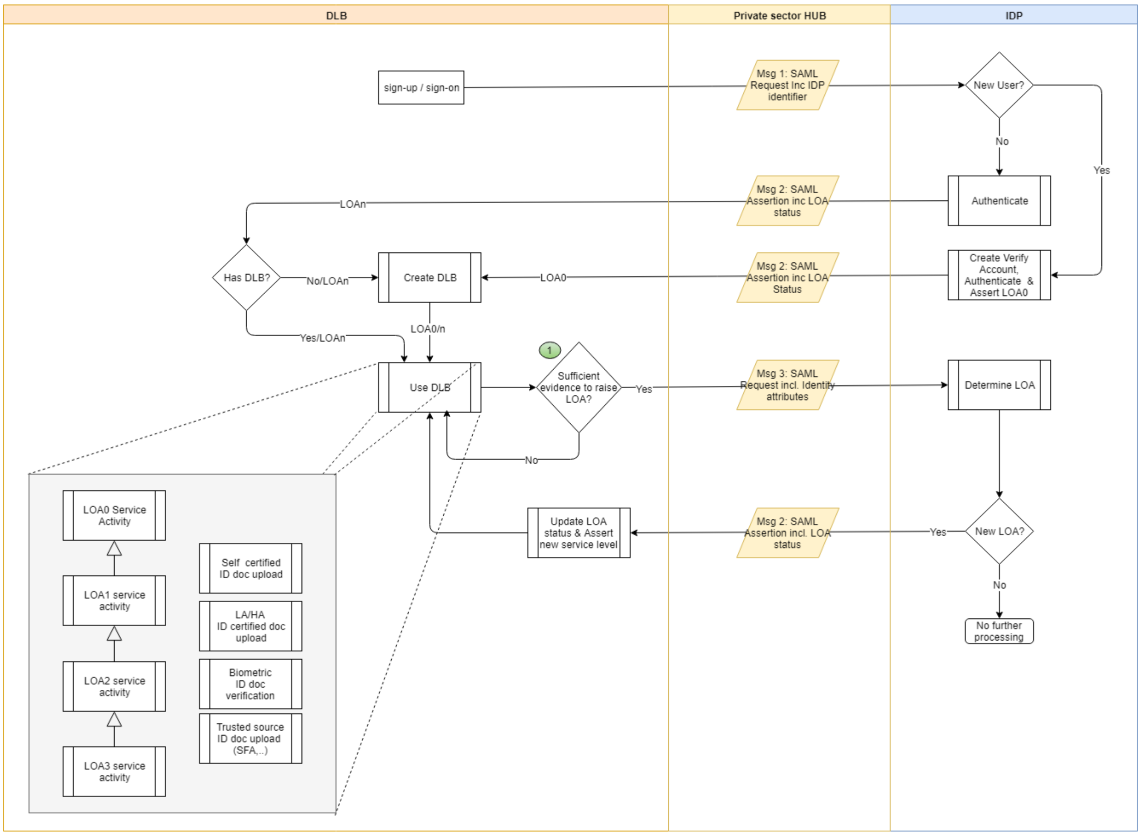
Citizen applies for a service.

Are they a new/existing customer, do they have a verified identity?

Diagram below indicates a potential workflow to help the citizen create a personal data store, upload information and get a verified identity, as part of a housing application process.

If they already have a personal data store their identity can be checked enabling them to progress with the job in hand.

Citizen can then choose to share key information with the service provider.


DLB
Private sector HUB
IDP
sign-up / sign-on
Msg 1: SAML Request Inc IDP identifier
New User?
No
Yes
Authenticate
Msg 2: SAML Assertion inc LOA status
LOAn
Has DLB?
No/LOAn
Create DLB
LOA0
Msg 2: SAML Assertion inc LOA Status
Create Verify Account, Authenticate & Assert LOA0
LOA0/n
Yes/LOAn
Use DLB
1
Sufficient evidence to raise LOA?
Yes
No
Msg 3: SAML Request incl. Identity attributes
Determine LOA
Update LOA status & Assert new service level
Msg 2: SAML Assertion incl. LOA status
Yes
New LOA?
No
No further processing
LOA0 Service Activity
LOA1 service activity
LOA2 service activity
LOA3 service activity
Self certified ID doc upload
LA/HA ID certified doc upload
Biometric ID doc verification
Trusted source ID doc upload (SFA,..)

Confirmed/Successful Application:

Other data will also be collected, typically from the local authority in question who might already hold data on the citizen.

Relevant data is uploaded through a Hub to the IDP.

IDP returns a level of assurance based on submitted data.

Level of assurances determines the person’s identity and eligibility for access to services.

Citizen achieves a successful housing application and becomes a successful customer of the local authority and/or housing association.

Based on their level of assurance a range of public services will be made available to them. If they have a low level of assurance e.g Level of Assurance 1 (LoA1) their level of assurance can be elevated over time to LoA2 enabling them to access more high value services, and carry out more complex online transactions, such as paying rent online or accessing other financial services.

Citizen can share different information at different times for access to other services. The more activity taking place through their personal data store will either help them elevate their level of assurance and /or ensure the continuity of their level of assurance and eligibility for access to public services. Continued activity also helps to ensure that the person is who they say they are, their information is factual and relevant to them, is not stolen or fraudulent and can be relied upon by service providers.