WHITE PAPER

Scottish Government DIS (OIA) – Sitekit Proof of Concept (PoC)

Jim Lound
Product Owner, Identity
Sitekit Systems Ltd
jim.lound@sitekit.net

Contents

1 Executive Summary

The Scottish Government Digital Identity Scotland Programme Board has the remit to deliver:

"A robust, secure and trustworthy mechanism by which an individual member of the public can demonstrate their identity online"

In support of this aim, Scottish Government engaged a number of partners to deliver PoC (Proof of Concept) digital identity functionality to enable assessment of modern technologies vis-à-vis their suitability for deployment at scale, across public services and for all citizens of Scotland.

Through this PoC, Sitekit has led the delivery of the underlying digital identity platform – an integration layer that enables rapid and straightforward "wiring-up" of digital services with identity providers and thereby providing service access to citizens.

1.1 Conclusions

Sitekit's PoC work demonstrated the following use-cases:

- User signs-in to North Lanarkshire demonstration application with their myaccount identity
- User signs-in to North Lanarkshire demonstration application with their Post Office identity
- User signs-in to Social Security demonstration application with their myaccount identity
- User signs-in to Sitekit third party test harness with their myaccount identity
- User sign-in to Sitekit third party test harness with their Post Office identity

Achievement of these use-cases also showing:

- Ease of integration and interoperability with digital public services (relying party applications):
  - Scottish Social Security
  - North Lanarkshire Council
- Ease of integration and interoperability with digital identity providers:
  - myaccount
  - Post Office
- Suitability of Microsoft Azure cloud technology, demonstrating:
  - Value for money
  - Ease of set-up and configuration
  - Security and resilience
  - Ability to scale

1.2 Recommendations

With the PoC work now complete Scottish Government should evaluate outcomes and set a clear plan for delivering a live service:

- Setting a phased delivery roadmap, potentially including a "Beta" programme of work, where end-end functionality is delivered
- Careful evaluation of digital public services in scope, ensuring that organisations engaged have the capability and desire to deliver value rapidly
- In digital service context, understand service user needs:
  - How they prefer to interact with digital services (at home or on the move; desktop PCs vs smartphone)
  - Digital identity on-boarding opportunities and challenges (users with an existing digital identity may want to bring this with them; new users)

- Setting clear success measures: services on-boarded, users on-boarded, **transactions completed online => money saved over telephone or face-face interactions**

1.3 Document Scope

This document summarises the involvement of Sitekit in the Scottish Government DIS (OIA) Proof of Concept during the key stages of the project. The key stages, from Sitekit's perspective, were:

- Proposed approach to a POC on Stream 1 of the Alpha Programme
- Initial design post Alpha kick off meeting
- Implementation resulting from further engagement with stakeholders

In addition, in this document Sitekit lays out an array of features and capabilities that we believe will satisfy the needs of citizens, service providers and Scottish Government alike. These features include:

- The ability to allow citizens to take advantage of the bring your own identity (BYOI) feature.
- The ability for the citizen to create a new digital identity with their chosen identity provider.
- Allow existing digital identities to be uplifted in assurance terms by the original identity provider.
- Allow existing digital identities to be uplifted by the Scottish Government's identity assurance service.
- Provision of a Scottish Government branded digital identity by the identity assurance service.
- To allow digital identities to be uplifted using a vouching service undertaken by the service provider, government entity or a private sector organisation.
- To allow personal entitlement attributes to be conveyed securely to the service provider.
- Facilitating single sign on whereby the citizen can move seamlessly and securely from one government service to another without having to log in again.

1.4 Acknowledgement

Sitekit thanks Scottish Government for the opportunity to participate in work done to date, and the readiness of PoC partners to engage and support. As a business founded and predominantly run in Scotland, delivering improved public services delivers real benefits for Sitekit staff, their families and friends. Sitekit welcomes the opportunity to work further with Scottish Government and deliver next-generation digital identity services for Scottish citizens.

2 About Sitekit

Sitekit's identity team includes 45 engineers based in London, Oxford, Edinburgh and the Isle of Skye. Founded in 1989, Sitekit first delivered communications technology for oil and gas, then moving into web development in the mid '90s. As this market matured, Sitekit developed its own content management system, Sitekit CMS, launching at CeBIT (Hanover) and proving an immediate hit.

Initially delivering a technology solution across sectors, in 2009 Sitekit focussed on delivering web solutions for the NHS – supported by the then Government's mandate for PCTs (Primary Care Trusts) to improve engagement and communication with patients. Sitekit grew market share to 80 NHS organisations and was the largest single supplier of web development services to NHS organisations.

Sector focus brought deeper knowledge of the challenges faced by health and care, and growing awareness of emergent "dHealth" initiatives – brought together with Innovate UK's (then Technology Strategy Board) dallas programme (delivering assisted living lifestyles at scale), a £37.5M fund to examine technical challenges in health and care and propose solutions with Sitekit working in each dallas project

NHS Liverpool CCG's dallas project, More Independent (Mi) initially focussed broadly on interoperability, then specifically on assured, digital, citizen identity – recognising that to move data between health and care systems, and into the realm of the citizen, an assured, digital, citizen identity is a pre-requisite. Sitekit and NHS Liverpool CCG delivered Alpha functionality in partnership with NHS Digital and NHS England to test both technical feasibility and user perceptions. In parallel, Sitekit leveraged its partnership with Microsoft to assess next-generation Azure technologies, working closely with Microsoft product group to deliver solutions to Microsoft Enterprise customers – including Nuffield Health, Bupa, Lloyd's Register and financial clients.

As subcontractor to Microsoft, Sitekit delivered DWP's EAS-Replacement service, supporting DWP's transition from Government Gateway to a modern and cost-effective solution. EAS-R is in live operation, with Sitekit providing both application development, and support services to DWP directly.

Today, Sitekit enjoys a pre-eminent position as a leading provider of digital identity to Government and enterprise clients.

3 Project Background

Sitekit has welcomed the opportunity to engage in the Scottish Government DIS (OIA) Proof of Concept and thereby being able to present the capabilities that Sitekit has to offer Scottish Government as a Microsoft Gold Partner utilising the Azure AD B2C cloud identity service.

Sitekit shares the Scottish Government's vision in relation to utilising the power of digital identities to help transform local and central government services in the digital world and being able to realise the significant benefits this will bring for citizens and service providers alike.

Critical to achieving this success is for all stakeholders to have confidence in the service that supports the use of digital identities and how they are created, maintained and utilised.

3.1 Service Providers

Service providers, such as Social Security Scotland, need to have confidence in the identity of the citizen accessing their services balanced with a seamless and productive user experience. Service providers do not want to see citizens dropping out of their process when they reach the identity assurance step.

Service providers need to able to efficiently onboard to an identity assurance service with a single technical connection giving access to multiple identity providers (IdPs) and receiving responses from identity providers converted into a standard format for easy consumption.

Digital identities are not just about proving identities, they also provide the key to unlocking the provision of additional personal attributes, for example those that relate to entitlement of service, in a secure and productive way. These additional attributes may be held by local and central government, by educational institutions and by the private sector, for example.

3.2 Citizen Perspective

From a citizen's perspective, being able to utilise an existing digital identity to conduct their business in a digital world is very important. It helps those individuals that want to minimise the number of user ids and passwords that they have to achieve this through the use of a ubiquitous capability to assert their identity using a digital identity. A digital identity makes the individual more productive online allowing both control over who receives their personal data in addition to making the provision of their personal data to a service much more effective and secure.

4 Scoping & Analysis

Prior to implementation, Sitekit undertook scoping and analysis activities to present implementation options to Scottish Government.

4.1 Proposed Approach

Based upon the output from the Discovery project, Sitekit responded with a proposed approach to a Proof of Concept (PoC) on Stream 1 of the Scottish Government OIX Digital Identity Alpha Programme, based on use cases for the creation and use of digital identities in the context of the Child Disability Allowance (cDLA) and the Single Person Council Tax Discount.

Sitekit proposed to create a series of authentication journeys on Microsoft Azure's AD B2C cloud identity service to satisfy the use cases and requirements outlined in the table below.

Stream Outline	
Relying Parties	• Social Security • A Local Authority (TBC)
Services	• Applying for cDLA (Social Security) • Applying for Single Person Council Tax Discount (Local Authority)
Use Cases	• First time applicants for cDLA requiring creation of digital identity (LoA2) • First time applicant of Council tax single person discount requiring creation of digital identity (LoA2?) • First time applicants for cDLA where person has digital identity created previously when applying for Council tax single person discount • First time applicants for Council tax single person discount where person has digital identity created previously when applying for cDLA
User Types	• People with identity evidence (passports, credit history) • People without conventional identity evidence ▪ Using face-to-face process at either Social Security or Local Authority ▪ Using face-to-face process at Post Office

Figure 1 - requirements response: PoC

These capabilities were presented in a manner designed to emphasise inclusiveness, user experience and user productivity in the following ways:

- Allowing the user to take advantage of the ability to 'Bring Your Own Identity', whereby an existing digital identity can be used to allow the user to assert their identity to Scottish Government. These BYOIs would include social media, GOV.UK Verify, myaccount.
- Enabling the user to create a new digital identity with an identity provider e.g. myaccount.
- Provision of a Scottish Government Digital Identity, whereby the user choses to uplift their social media identity and create a new Scottish Government Digital Identity with credentials appropriate to the required level of assurance. The Scottish Government Digital Identity could be explicitly Scottish Government branded or the higher level of assurance and new credentials could be associated with the user's social media account within the Scottish Government Sitekit Identity Assurance Platform on behalf of Scottish Government.

- Allowing users to create a new Scottish Government Digital Identity without using an existing digital identity as the starting point or to create a new Scottish Government Digital Identity having asserted their identity with an existing digital identity of the equivalent level of assurance.
- Facilitating a Vouching service whereby a user can elect to attend a physical location in order to present their physical identity evidence as part of an identity uplift process or to complete an identity registration that was initially started online. The physical locations would be chosen by Scottish Government but, as examples, could include a Social Security office, a North Lanarkshire service point and Post Offices.
- Allowing the user to uplift the level of assurance, associated with a BYOI, in the online journey in order to satisfy the service provider's requirements as the Relying Party (RP). The RP's level of assurance requirements will reflect the level of risk associated with the transaction and the associated degree of confidence needed in the user's identity. Additionally, an RP may, for a single transaction, have a number of discrete steps that incrementally require a higher level of assurance (LoA) as the user progresses. For example, the user may only require an LoA0 to initiate the process but needs to start the final stage with an LoA2. For social media identities and Scottish Government identities, the uplift would be undertaken within the Scottish Government Sitekit Identity Assurance Platform and the credentials, appropriate to the level of assurance, would be issued through the platform. For existing identities associated with Verify & myaccount for example, the uplift of the level of assurance and credentials would be carried out by the relevant IdP via the Scottish Government Sitekit Identity Assurance Platform.
- The Scottish Government Sitekit Identity Assurance Platform would also support the provision of attributes to the RP with the user's express consent where these attributes could be source from the user's IdP, personal data store or other third-party sources.

4.2 User Journeys

As a straw man, Sitekit proposed the following user journeys whereby in 1 & 2 the user would start with a social media identity and be uplifted through Vouching to create a Scottish Government LoA2 identity. In journey 3 & 4, the user would start with an existing LoA2 identity and assert their identity to the RP with a question around whether a Scottish Government identity would be created on the back of this. In journeys 5 & 6, the user is asserting their identity using an existing Scottish Government identity.

Journey Number	Starting with	Uplifted by	Creating	Accessing
1	Social IdP	Vouching	Scottish Government Digital ID LoA2	Social Security cDLA
2	Social IdP	Vouching	Scottish Government Digital ID LoA2	Local Authority SPD-CT
3	myaccount LoA2	N/A	?	Social Security cDLA
4	Post Office Verify LoA2	N/A	?	Local Authority SPD-CT
5	Scottish Government Digital ID LoA2	N/A	N/A	Social Security cDLA
6	Scottish Government Digital ID LoA2	N/A	N/A	Local Authority SPD-CT

Figure 2 – proposed user journeys

4.2.1 Journey Diagrams

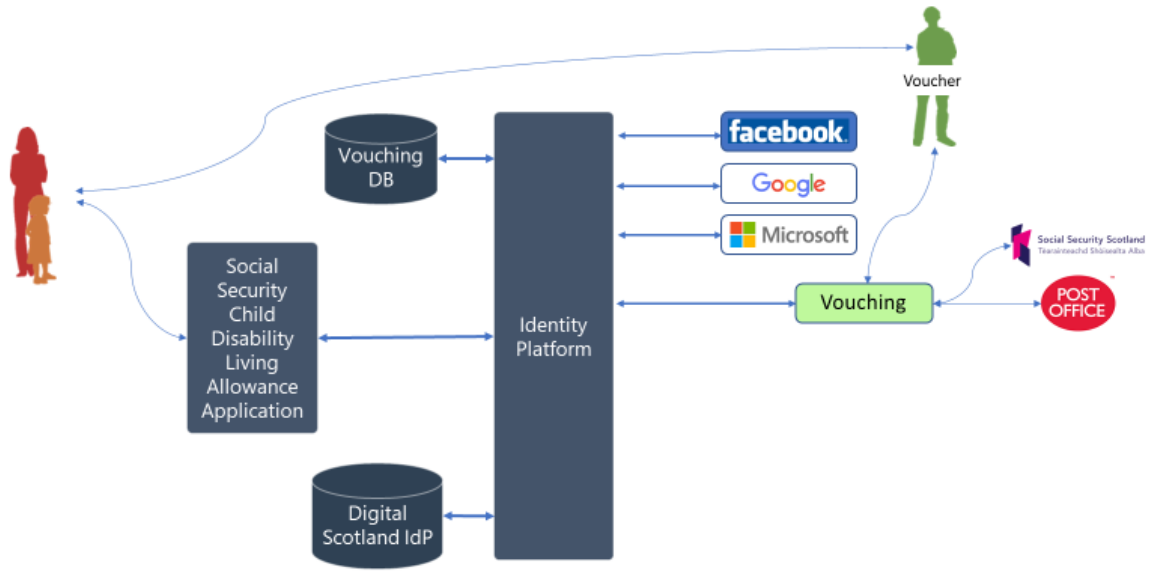

Figure 3 - journey one: LoA2 identity via social identity provider and vouching, cDLA

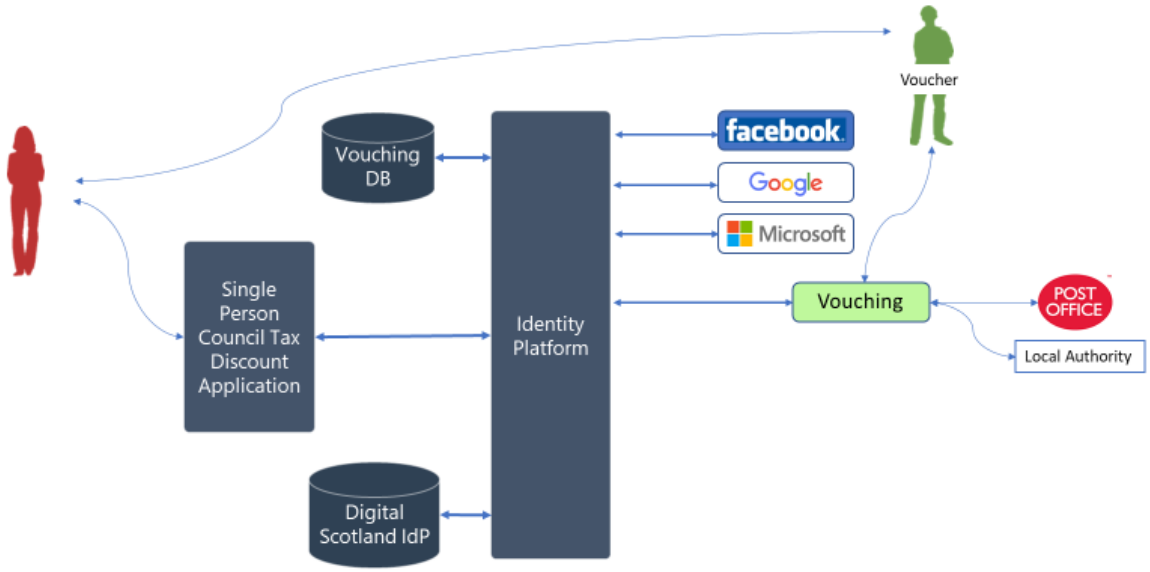

Figure 4 - journey two: LoA2 identity via social identity provider and vouching, SPD-CT

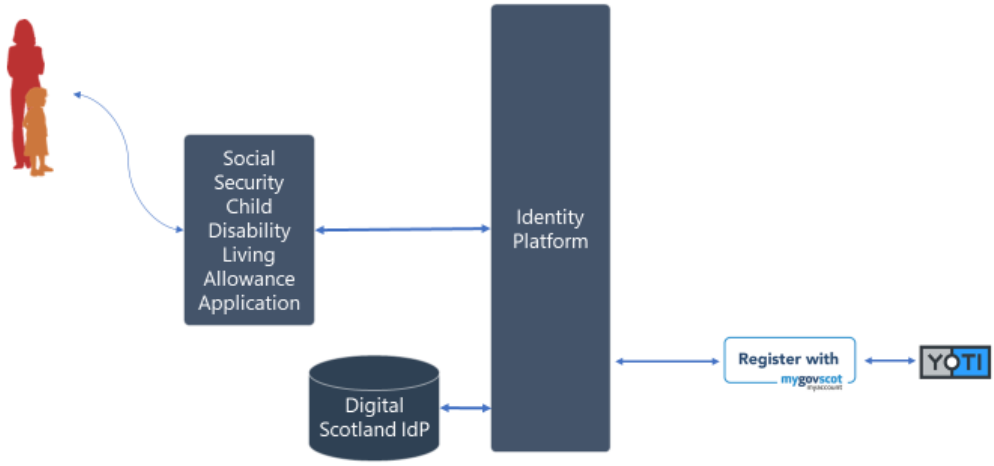

Figure 5 - journey three: LoA2 identity via myaccount and YOTI, cDLA

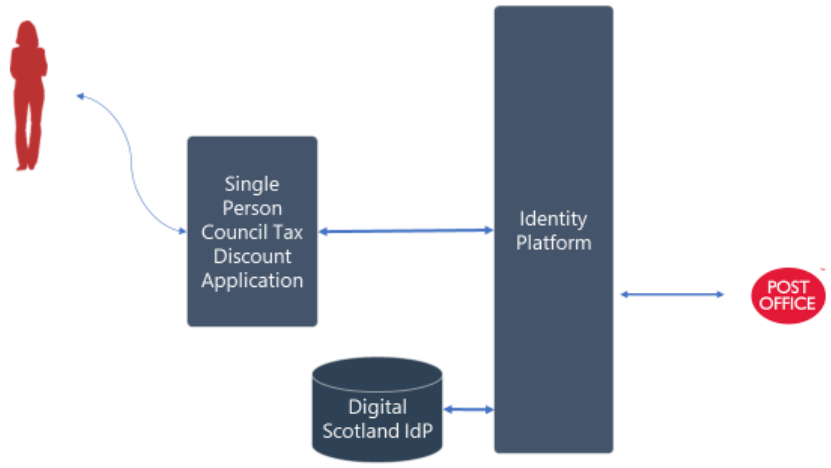

Figure 6 - journey four: LoA2 identity via Post Office, SPD-CT

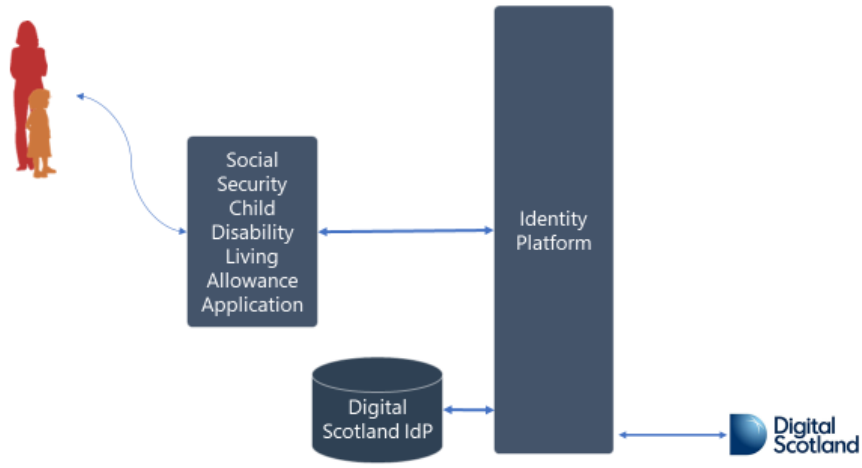

Figure 7 - journey five: LoA2 identity via Digital Scotland, cDLA

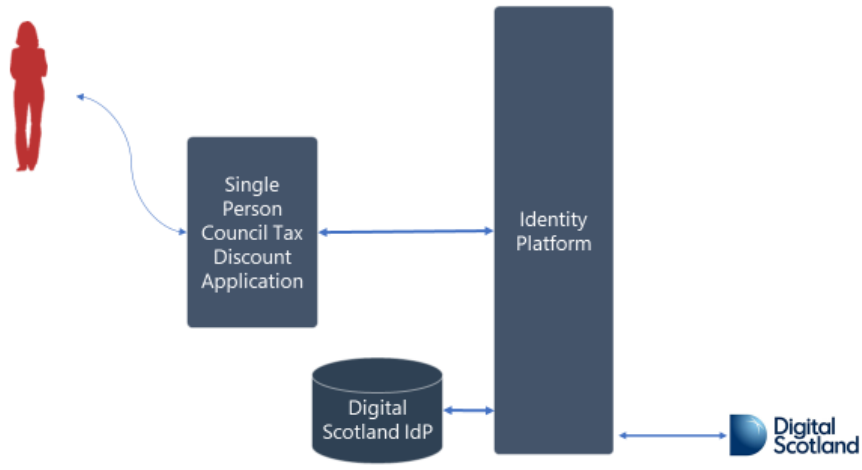

Figure 8 - journey six: LoA2 identity via Digital Scotland, SPD-CT

5 PoC Objectives & Roadmap

Extract below re-states Scottish Government PoC (Alpha) objectives:

5.1 Objectives

The aim of this Alpha is to test the proposed OIA approach through the development of a prototype, undertaking a gap analysis and performing user research to:

- *Test the architectural approach and the ability of providers in the market to support it*
- *Assess how best to achieve a good enough level of standardisation and interoperability identity services, for Scottish public services*
- *To test the resultant user experience with real customers*
- *To test integrating the approach into public service user journeys*

The project should support the testing of a sufficiently wide range of user journeys including:

- *Entry into the digital identity system from multiple places*
- *Users with multiple needs*
- *Different types of public service – and by implication different requirements*

5.2 Stream 1: Proof of Concept

- ***Scope**: This stream will build a PoC to test use cases for the creation and use of digital identities in the context of DLA Child and the Single Person Council Tax Discount.*
- ***Relying Parties**: Social Security, Local Authority*
- ***IDPs**: GOV.UK Verify IDP, an alternative IDP and a provider of verified attributes*
- ***Services**: Applying for DLA Child, Applying for Single Person Council Tax Discount*
- ***Use cases**: Range of user journeys*
- ***User types**: People with and without conventional identity evidence*

5.3 Platform User Flows

The Scottish Government Sitekit Identity Assurance Platform is built using the Microsoft Azure AD B2C cloud identity service. Scottish Government would have its own Azure subscription. Sitekit itself would not hold any Scottish Government related data.

The user flows would be initiated by user activity at the Relying Party end where the RP would engineer the identity assurance step into their process. At the appropriate step in the RP process, the user would be invited to choose how they want to prove their identity to the RP. Within the identity assurance part of the flow, Sitekit would receive the request, identify the user's chosen identity provider and return the user to the RP.

The range and number of journeys before and after the identity assurance step is immaterial to the identity assurance step. There would be a defined number of journeys through the identity assurance step supporting a range of RP journeys. As an example, this concept is reflected in the five central arrows in the diagram below:

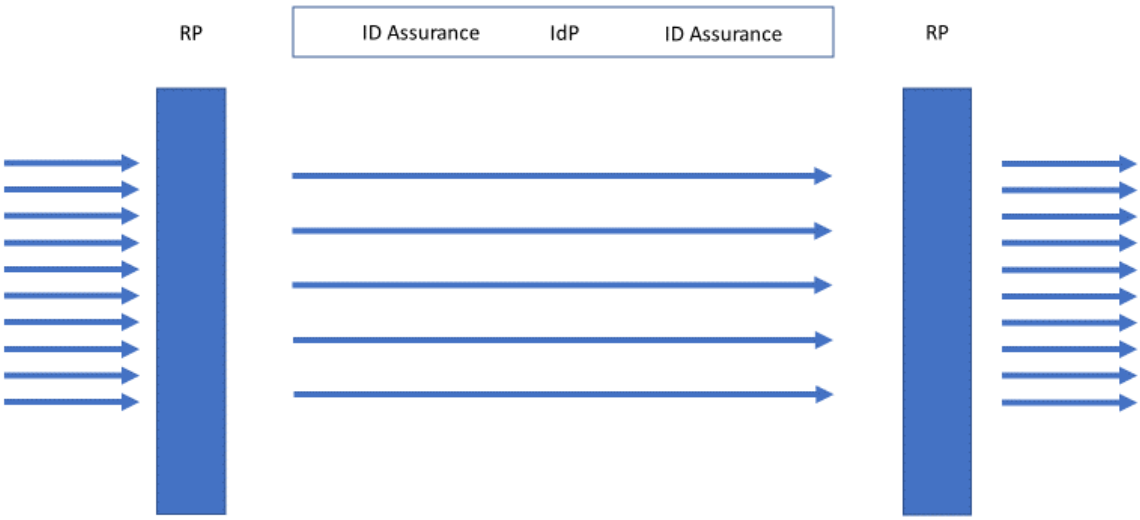

Figure 9 - relying party vs identity assurance interactions

5.3.1 Use Cases & Phasing

Following Scottish Government engagement use-cases were refined with respect to project phase:

Phase #	Use Case #	RP service step #	Starting with BYOI	Starting LoA	LoA required by RP	Uplifted by	Creating	Data to be returned
1	1	N. Lan #?	Post Office	LoA1	LoA1	N/A	N/A	PO MDS
2	2	Soc Sec #?	Post Office	LoA2	LoA2	N/A	N/A	PO MDS
	3	Soc Sec #?	Post Office	LoA1	LoA2	PO IdP	N/A	PO MDS
3	4	N. Lan #?	myaccount	LoA1	LoA1*	N/A	N/A	myaccount MDS
4	5	Soc Sec #?	myaccount	LoA1	LoA2*	RP Vouching	IA Record	myaccount MDS + self asserted PII
					*In this scenario a Scottish Govt LoA will satisfy the RP			

Figure 10 - use cases vs project phase

- For phase 1 (use case 1) it was proposed to introduce a single Relying Party (North Lanarkshire) and a single IdP (Post Office)
- For phase 2 (uses cases 2 & 3) it was proposed to add in the second RP (Social Security) utilising the existing IdP and to introduce an uplift step where the user already had a Post Office LoA1 but the RP required LoA2.
- For phase 3 (use case 4) it was proposed to add in myaccount as the second IdP.
- For phase 4 (use case 5) it was proposed to introduce an uplift from a myaccount LoA1 to an LoA2 through introducing a vouching process undertaken at a Social Security office. It was also proposed to introduce the ability for the user to add in self-asserted attributes for consumption by the RP (e.g. self-asserted National Insurance Number).

Reference to MDS relates to the user's PII held within the Matching Data Set that the IdP will have available for an RP to request. The RP can request MDS elements that are appropriate for the RP transaction subject to consent by the user.

5.3.2 Use Case Five

Use case five illustrates identity assurance capabilities:

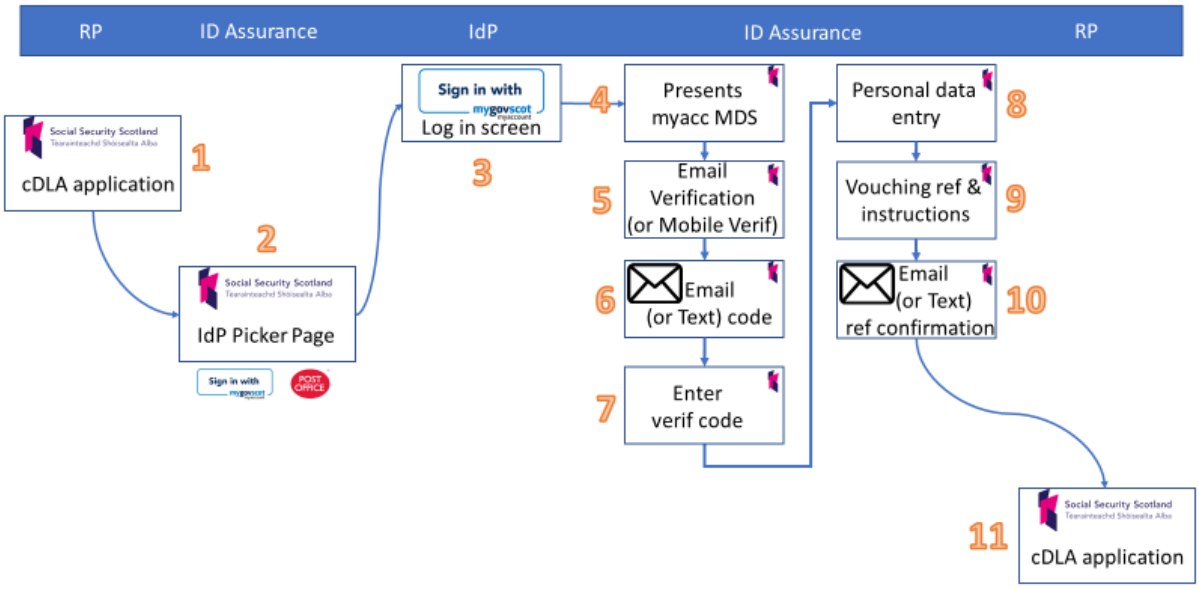

Figure 11 - use case five, myaccount sign-in

1. Represents the user's first visit to the RP and at the point in the RP process when the user is requested to prove their identity the user is re-directed to the Scottish Government Sitekit Identity Assurance Platform.
2. User is presented with the IdP picker page relevant to Scottish Government. The user selects myaccount and is re-directed to myaccount.
3. User logs in using their myaccount credentials and is re-directed to the Scottish Government Sitekit Identity Assurance Platform.
4. User is then presented with their myaccount matching data set (MDS).
5. As part of the uplift process the user is asked to verify their email address in order to engage with the Vouching process. The user enters their email address. [NB: as an alternative the user could verify their mobile instead].
6. User receives a code via email.
7. User enters their code to verify their email.
8. User may be asked to enter additional personal details to support the Vouching process. If self-asserted attributes are requested, the user can enter additional personal details.
9. User is presented with the Vouching instructions in terms of what to do next.
10. User receives an email containing the Vouching reference number to take to the physical location.
11. User is returned back to the RP.

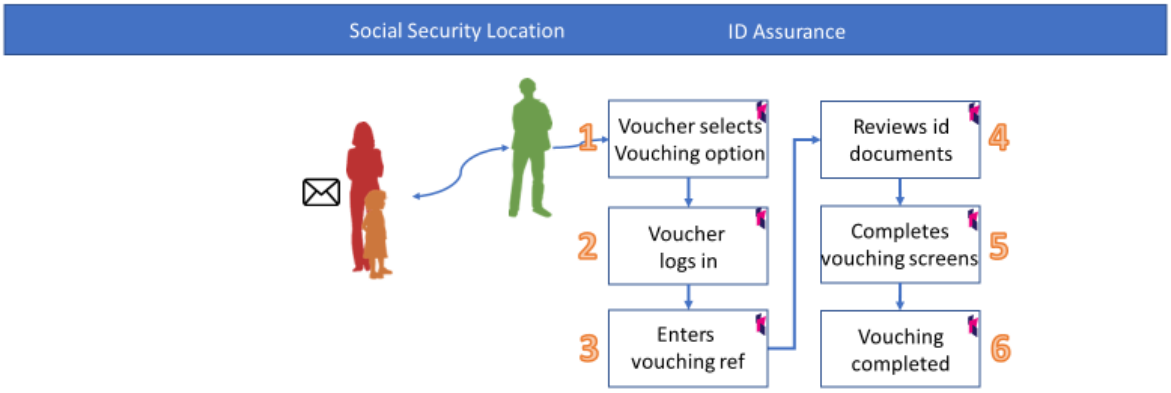

Figure 12 - use case five, vouching

1. On arrival of the user at the Vouching location, the Voucher selects the Vouching process on the menu
2. Voucher logs into the Vouching system.
3. Voucher enters the user's reference number.
4. Voucher reviews the identity documentation provided by the user and the user's personal data displayed on the Voucher's screen.
5. Voucher completes the Vouching process.
6. User is advised that the Vouching process has been completed and the user leaves the location.

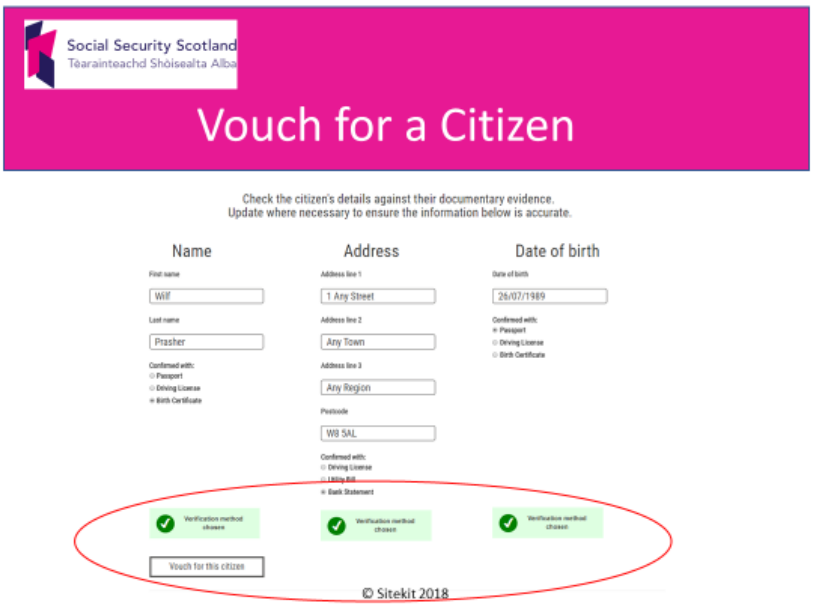

Figure 13 - vouching identity proofing

The Vouching system will reflect the specific requirements of the RP in terms of the minimum evidence requirements. The Voucher will review the identity evidence presented by the users and compare this

to the personal data displayed on the screen. The types of evidence accepted and the attributes that need to be confirmed are defined by Scottish Government to match their own identity proofing requirements. This is not prescribed by Sitekit.

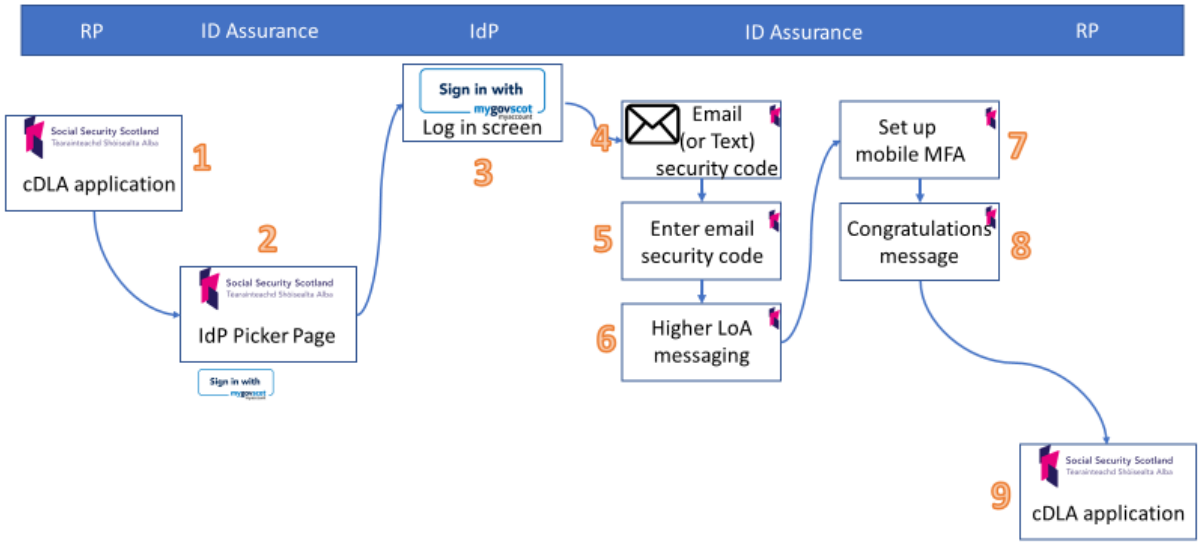

Figure 14 - service access following vouching

1. After the Vouching process, the user, at their convenience, returns online to the RP application. At the appropriate step in the RP process the user is redirected to the Scottish Government Sitekit Identity Assurance Platform.
2. User selects myaccount from the IdP picker page and is re-directed to myaccount.
3. User logs in using their myaccount credentials and is redirected to the Scottish Government Sitekit Identity Assurance Platform.
4. User is sent a code to their email.
5. User receives the code and enters it into the Scottish Government Sitekit Identity Assurance Platform. This binds the user to the higher level of assurance created via the Vouching process.
6. User sees the RP's 'level of assurance uplift' messaging and a request to set up a higher strength credential to match the higher level of assurance (in this example mobile MFA). NB: this may have already been set up earlier in figure 11 step 5.
7. User enters their mobile number, receives a text with a code and enters the code into the Scottish Government Sitekit Identity Assurance Platform to finish setting up the mobile MFA credential.
8. User sees a 'congratulations' message to confirm their success.
9. User is redirected back to the RP.

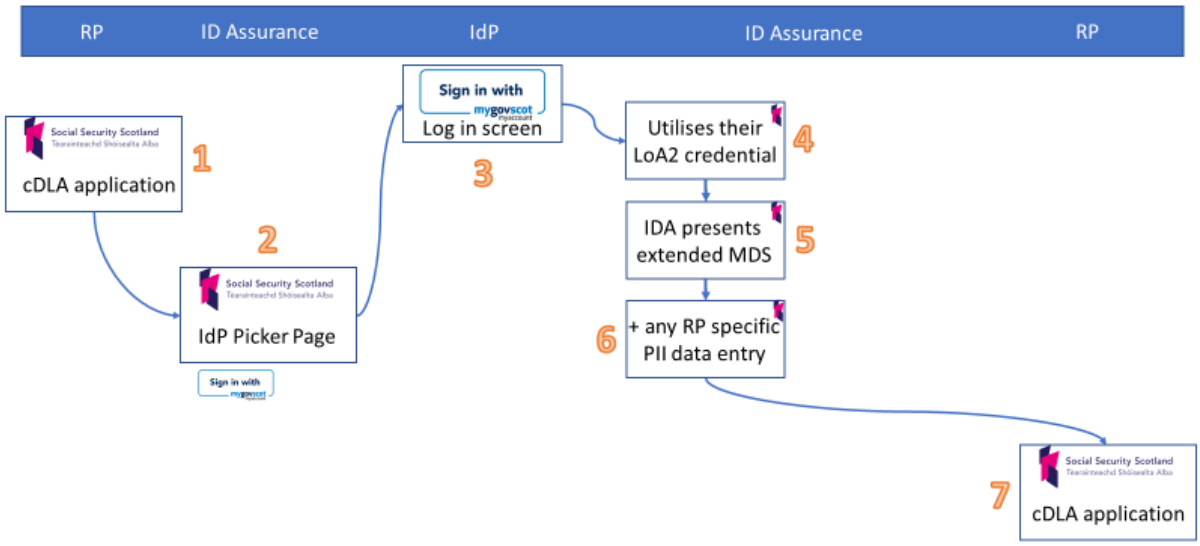

Figure 15 - service access on subsequent visits to the RP

1. On subsequent visits to the RP, at the appropriate point in the RP process when the user needs to assert their identity, the user is re-directed to the Scottish Government Sitekit Identity Assurance Platform.
2. User selects myaccount from the IdP picker page and is re-directed to myaccount.
3. User logs in using their existing myaccount credentials and is re-directed to the Scottish Government Sitekit Identity Assurance Platform.
4. Request for the higher strength credential required to satisfy the RP's higher level of assurance is triggered. The user receives a code via a text message and enters the code.
5. User sees the personal data associated with their myaccount MDS and their Scottish Government Sitekit Identity Assurance attributes requested by the RP. The user consents to their data being returned to the RP as appropriate.
6. RP has the oppportunity to request additional attributes that may be, for example, associated with the particular stage the user has reached within the RP process. The user enters the data as appropriate and consents to this data being returned to the RP.
7. User is redirected back to the RP.

5.3.3 Design Flows

The following represents a view of what would be happening within the Scottish Government Sitekit Identity Assurance Platform where the user journey is to utilise an existing Post Office identity which satisfies the level of assurance required by the RP.

At the point in the RP process, where the user needs to prove their identity, the user is re-directed via their browser to the IdP picker page in the Scottish Government Sitekit Identity Assurance Platform. At the same time the RP sends a request that defines the minimum requirement in terms of the level of identity assurance and personal data to be returned. The user selects (in this example) the Post Office as their chosen IdP. If the user does not have an existing Post Office identity, the user can register for one at this point in the process.

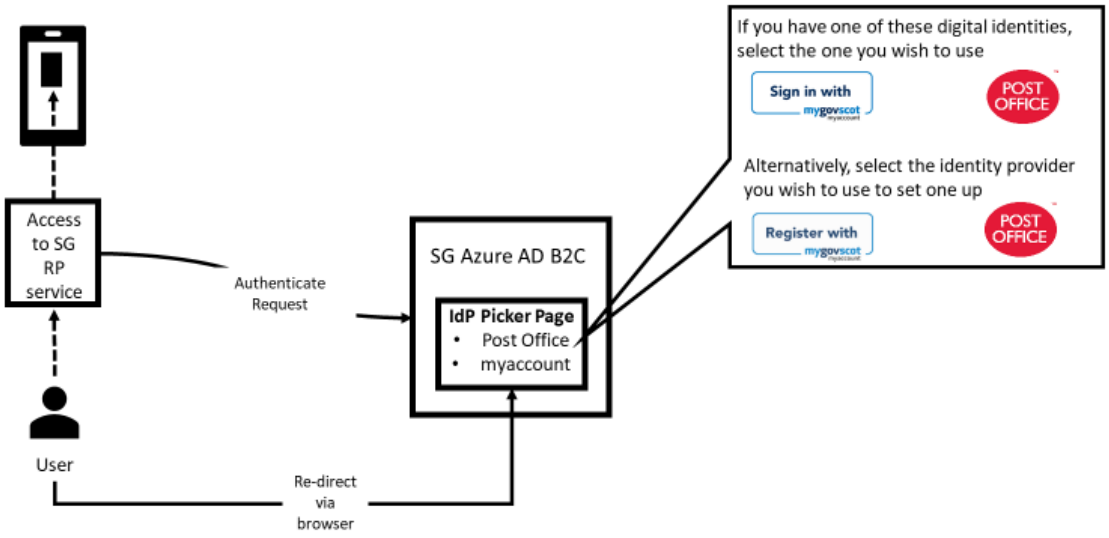

Figure 16 - design flow, authentication request

In order to enable the RP to have a single authenticate request format (a single pipe into the IdPs onboarded) the Scottish Government Sitekit Identity Assurance Platform effectively becomes the RP from the IdP's perspective. The user is re-directed to their chosen IdP. The IdP receives the authenticate requests. The user logs into the IdP and consents to their data being returned to the RP

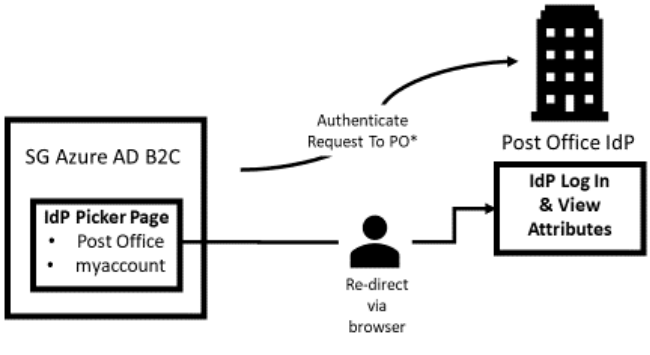

Figure 17 – design flow, authentication orchestration

The Scottish Government Sitekit Identity Assurance Platform receives the response from the IdP. The Scottish Government Sitekit Identity Assurance Platform sends the response to the RP in the format expected by the RP thereby supporting the principle of a ‘single pipe in’ and a ‘single pipe out’ which provides significant benefits to the RP.

In addition, the IdP has a ‘single pipe’ to return their responses to a range of RPs onboarded to the Scottish Government Sitekit Identity Assurance Platform.

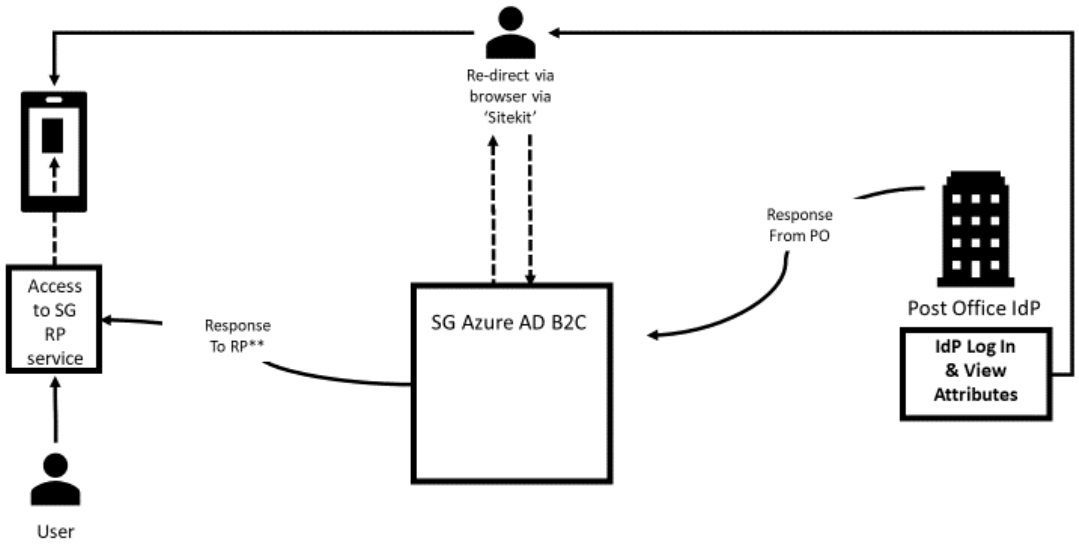

Figure 18 - design flow, authentication response

6 PoC Implementation

As the PoC progressed and requirements were elaborated the following identity assurance configuration was implemented:

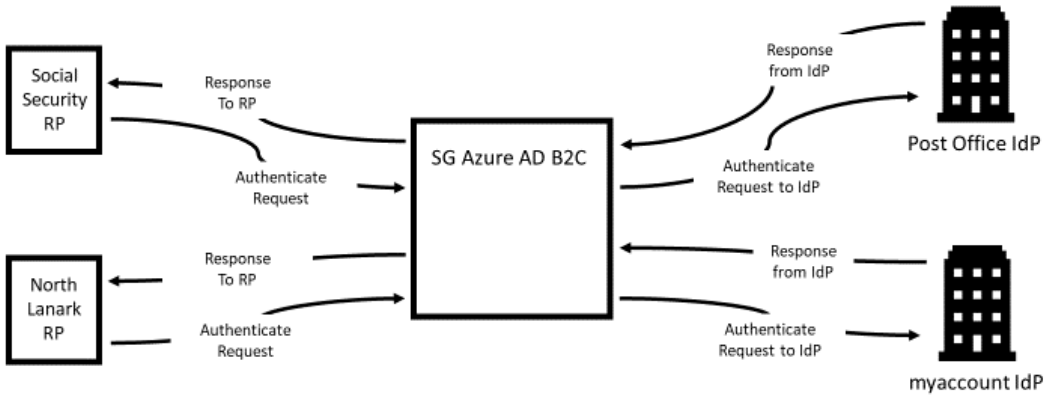

Figure 19 - design flow, PoC scope

6.1 Conceptual Architecture

Conceptually, the platform is illustrated:

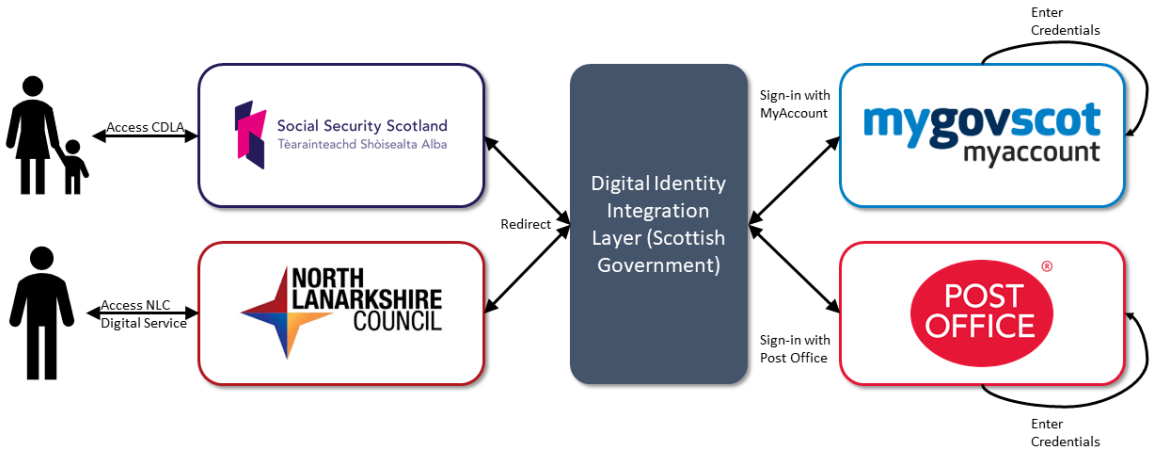

Figure 20 - digital identity platform conceptual architecture

- Social Security Scotland and North Lanarkshire Council represent **Relying Party Applications** – digital services that need an assured digital identity to enable a user to transact online

- myaccount and Post Office represent **Identity Providers –** digital services that offer citizens an assured digital identity
- Digital Identity Integration Layer (Scottish Government) represents identity orchestration capabilities between relying party applications and identity providers (scope of work delivered by Sitekit):
  - Which IdPs are available to the user to choose in relation to each RP service
  - The ability to register for a new digital identity with the IdPs
  - The ability to log in with an existing identity with the IdPs

6.2 Logical Architecture

Logically, the platform is illustrated:

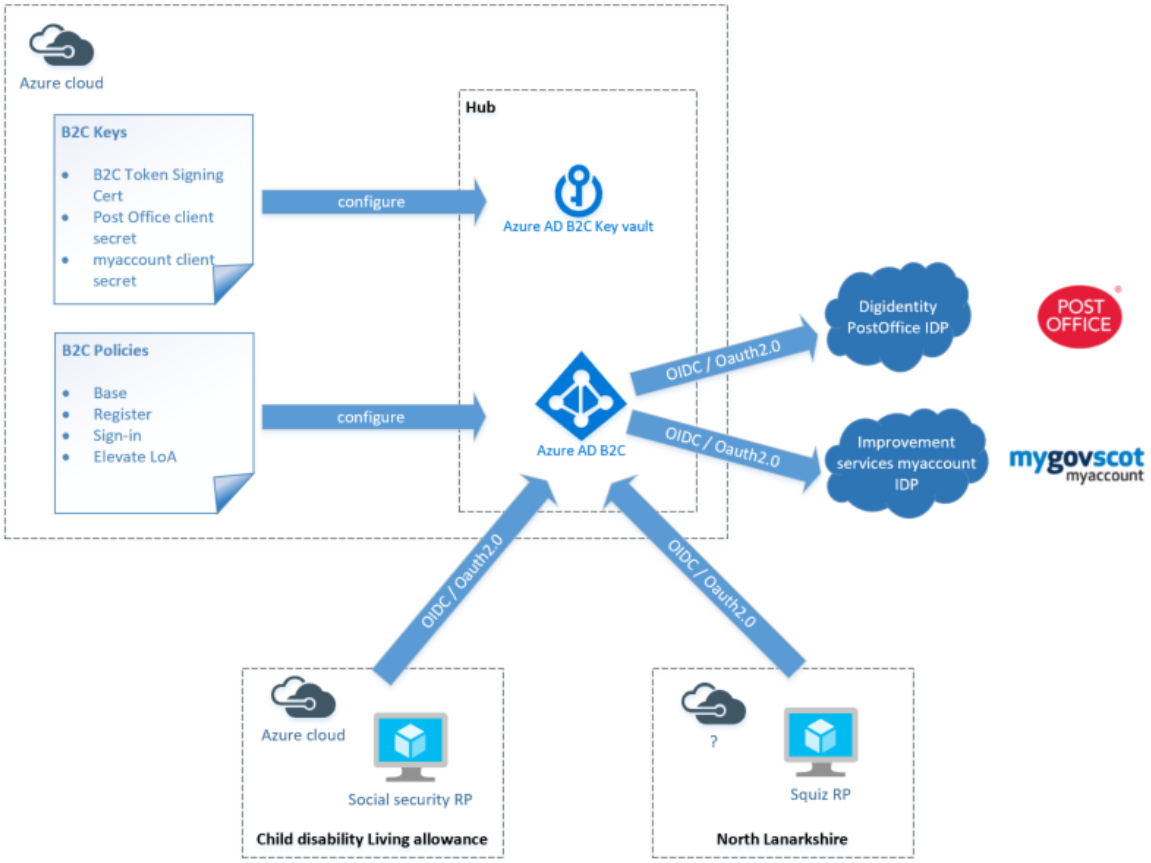

Figure 21 - logical architecture

- **B2C Policies** - refers to the policies that define the orchestration steps for each journey associated with the Social Security cDLA service and the North Lanarkshire Council portal (e.g. register and sign-in) and how they interact with the IdPs. It also defines how claims are managed internally and externally via tokens.
- **B2C Keys** – handles the security aspects associated with connections, policies and claims. These include any secrets, keys or certificates required for:
  - RPs to interact with B2C

- Policies interacting with identity providers
- B2C to issue token back to the RPs.
- Any other dependant APIs or services that need a secure interaction in the future.

- **Azure AD B2C** - this extends a standard Azure AD by adding the B2C Identity Experience Framework (IEF) capabilities on top. This allows B2C RPs to be defined, as well as the policies or journeys they can invoke, which is all managed through the standard Azure Management Portal.
- **Azure AD B2C Key Vault** – this is a cloud-based service providing data security and the ability to implement policies to regulate access to applications. The FIPS 140-2 Level 2 validated hardware security modules (HSMs) used to store B2C keys within Azure AD B2C.
- **OIDC / OAuth2.0** – the OIDC (Open ID Connect) extends OAuth2.0 to be used as an authentication protocol. It supports Single Sign On which allows users to seamlessly move between RP services in the same session. OIDC introduces the concept of an ID token which allows the identity of another party to be verified.
- **Social Security RP** – the Child Disability Living Allowance is the service utilising the POC from Social Security Scotland.
- **Squiz RP** – represents the North Lanarkshire Council portal utilising the POC.
- **Digidentity / Post Office IdP** – represents the Post Office's digital identity service operated by Digidentity.
- **Improvement Service's myaccount IdP** – represents the myaccount digital identity service.

6.3 Journeys Delivered

Sitekit delivered the following journeys through PoC implementation:

6.3.1 User signs-in to North Lanarkshire demonstration application (Squiz Portal) with their myaccount:

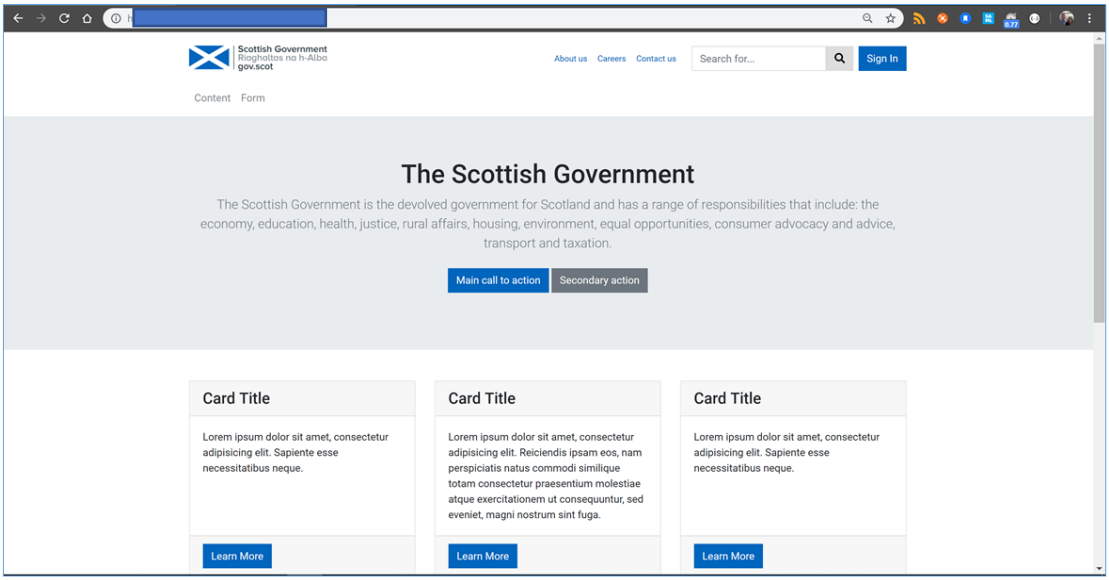

Figure 22 - user navigates to the Squiz portal and selects Sign In

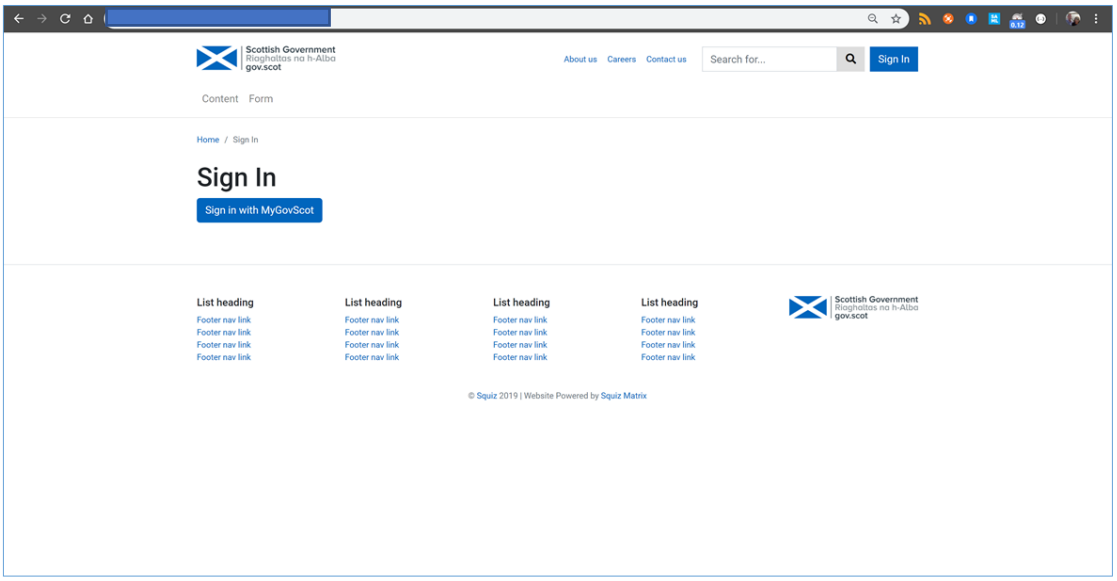

Figure 23 - user selects Sign in with myaccount

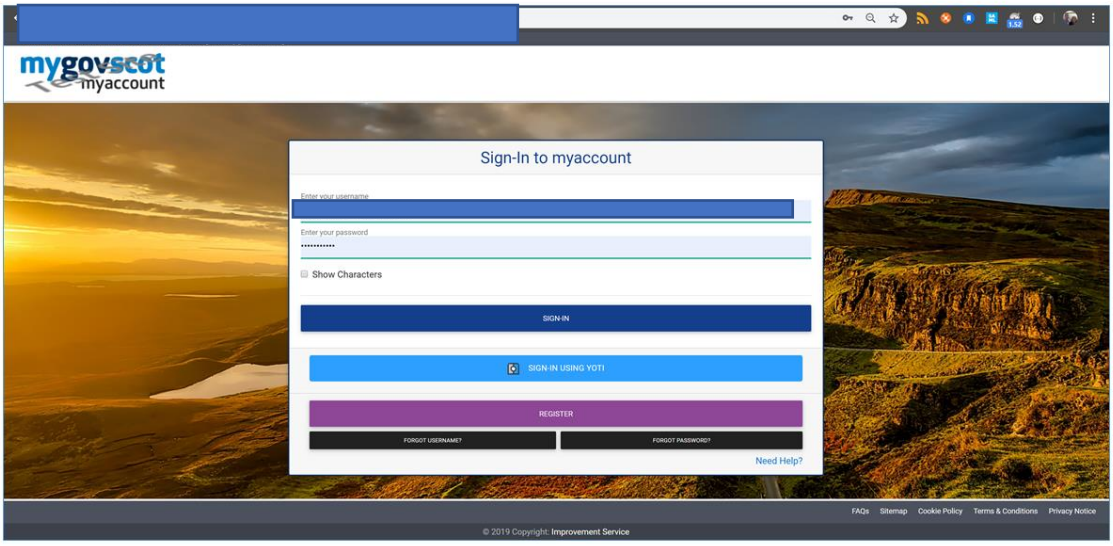

Figure 24 - user is redirected to myaccount sign in page and enters their credentials

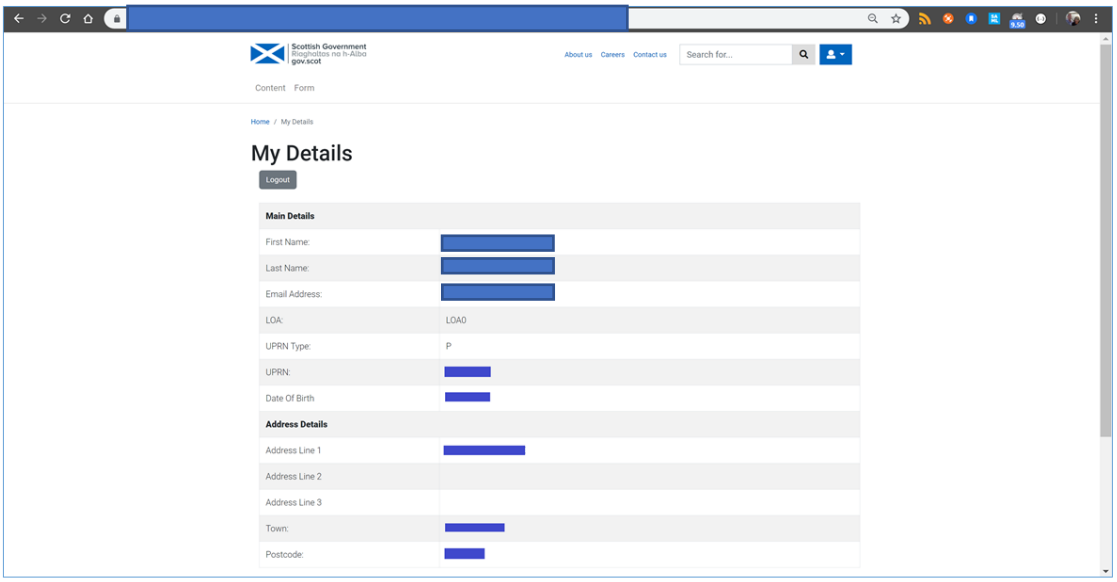

Figure 25 - identity attributes (claims) are returned from myaccount, via digital identity integration layer, for consumption by digital public service (Squiz portal)

6.3.2 User signs-in to demonstration application with their Post Office identity:

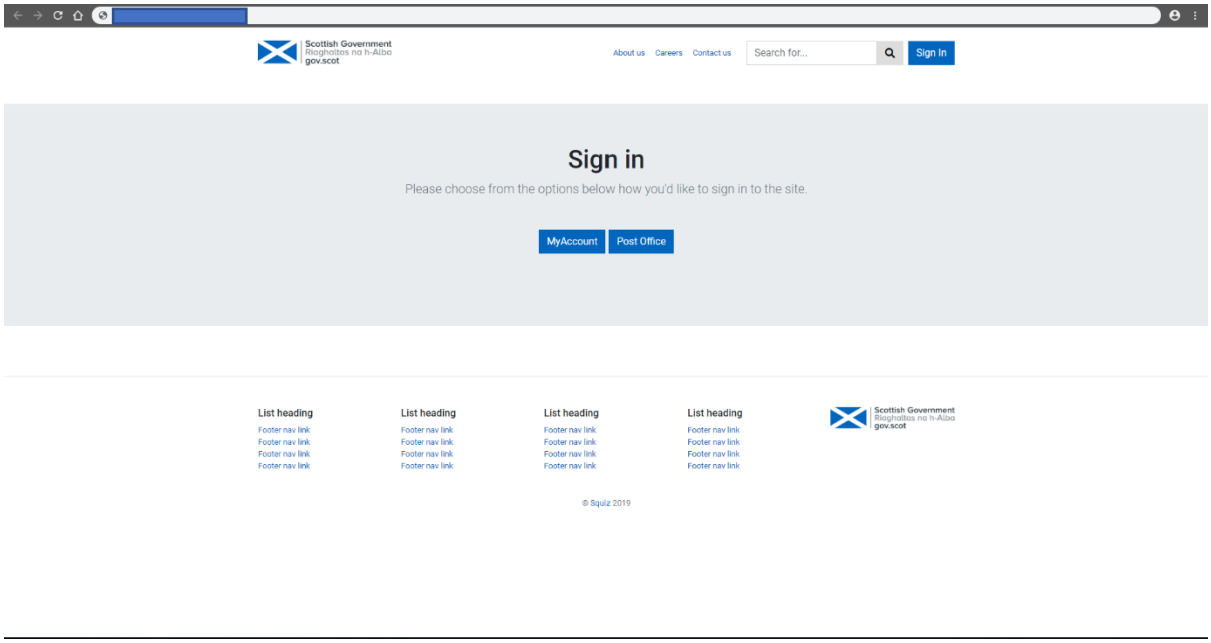

Figure 26 - user navigates to demonstration application and selects sign-in with Post Office

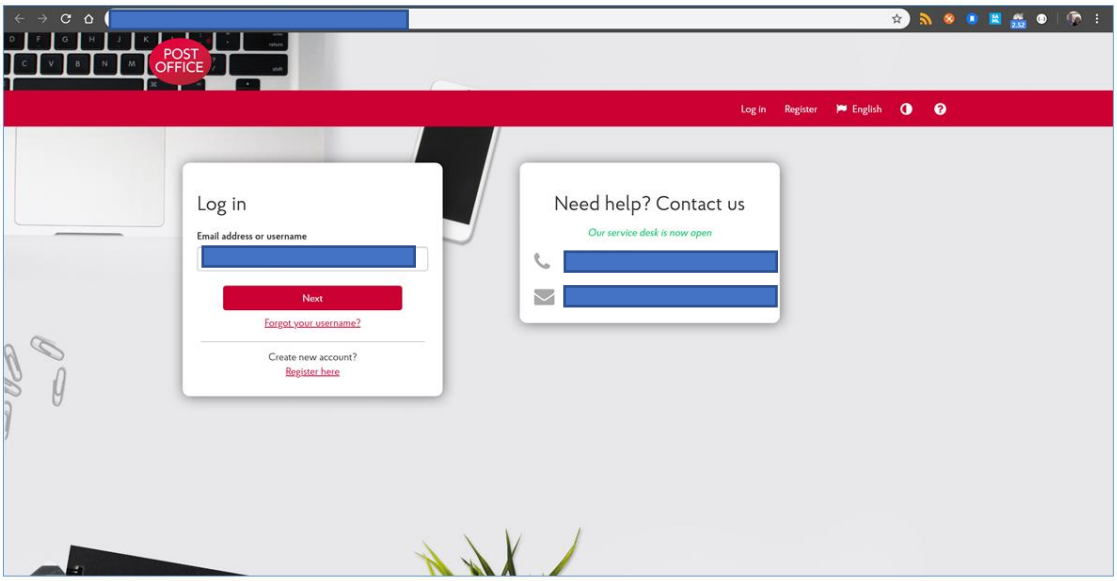

Figure 27 - user is redirected to Post Office sign-in page, enters their username

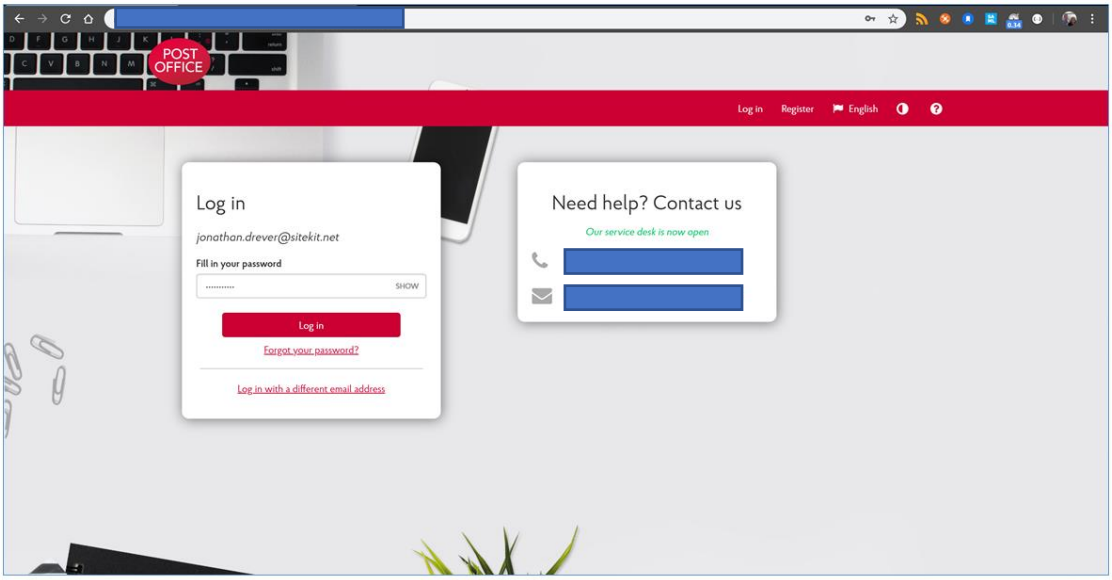

Figure 28 - user is requested to enter their password

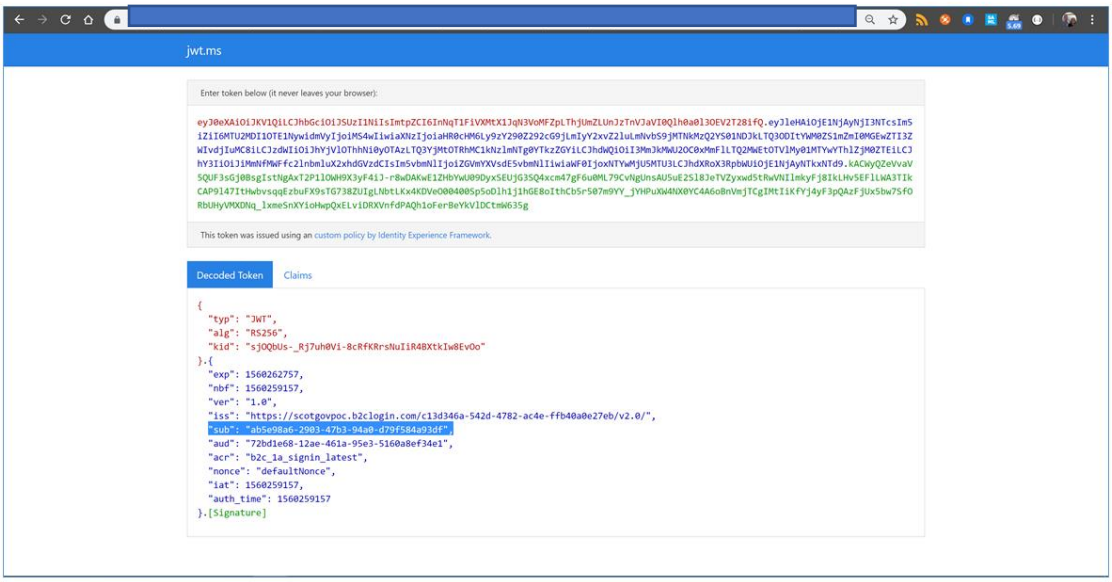

Figure 29 - identity attributes (claims) are returned from Post Office, via digital identity integration layer, for consumption by digital public service

6.3.3 User signs-in to social security demonstration application with their myaccount:

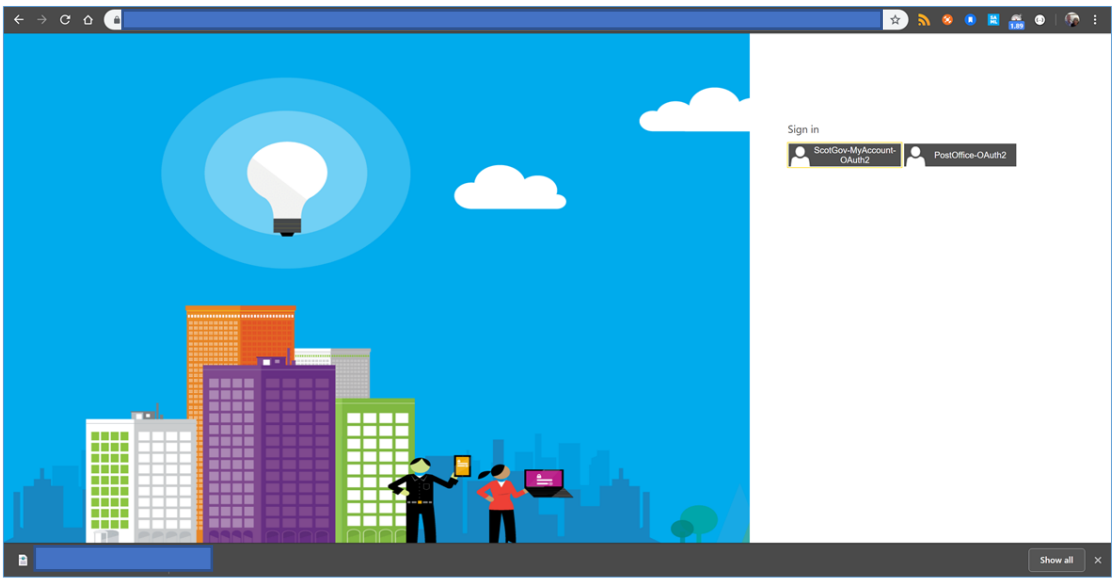

Figure 30 - user navigates to demonstration application and selects sign in with myaccount

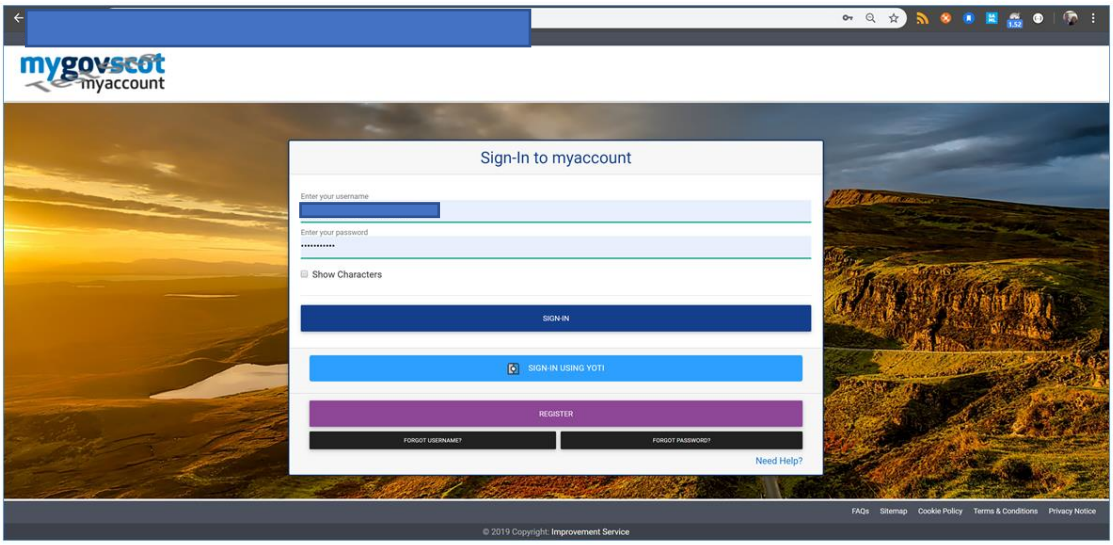

Figure 31 - user is redirected to myaccount sign-in page, enters their credentials

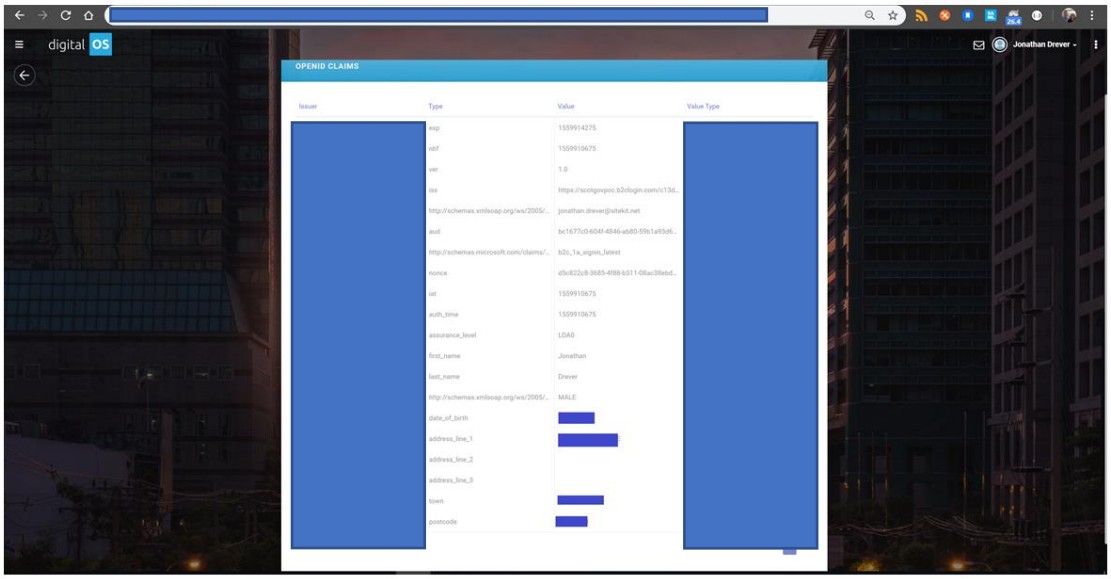

Figure 32 - identity attributes (claims) are returned from myaccount, via digital identity integration layer, for consumption by digital public service (social security demonstration application)

6.3.4 User signs-in to demonstration application with their myaccount identity:

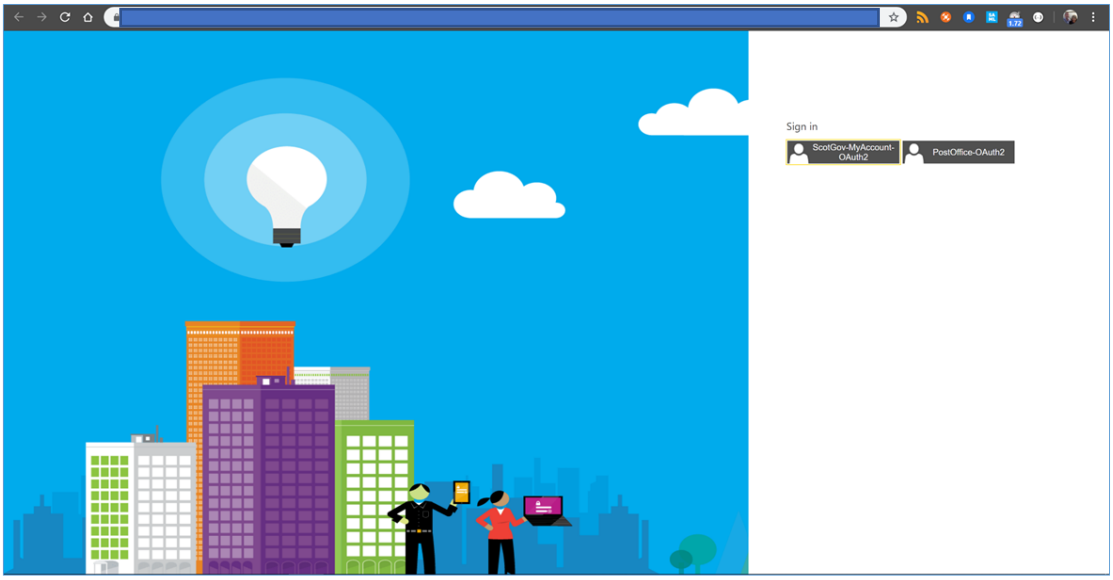

Figure 33 - user navigates to demonstration application and selects sign-in with myaccount

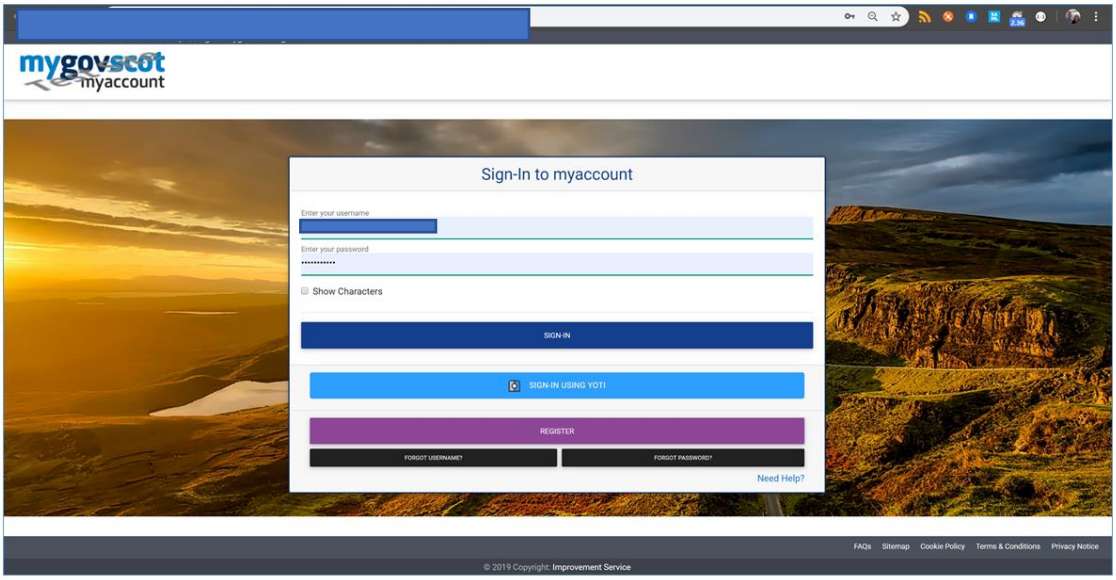

Figure 34 - user is redirected to myaccount sign-in page, enters their credentials

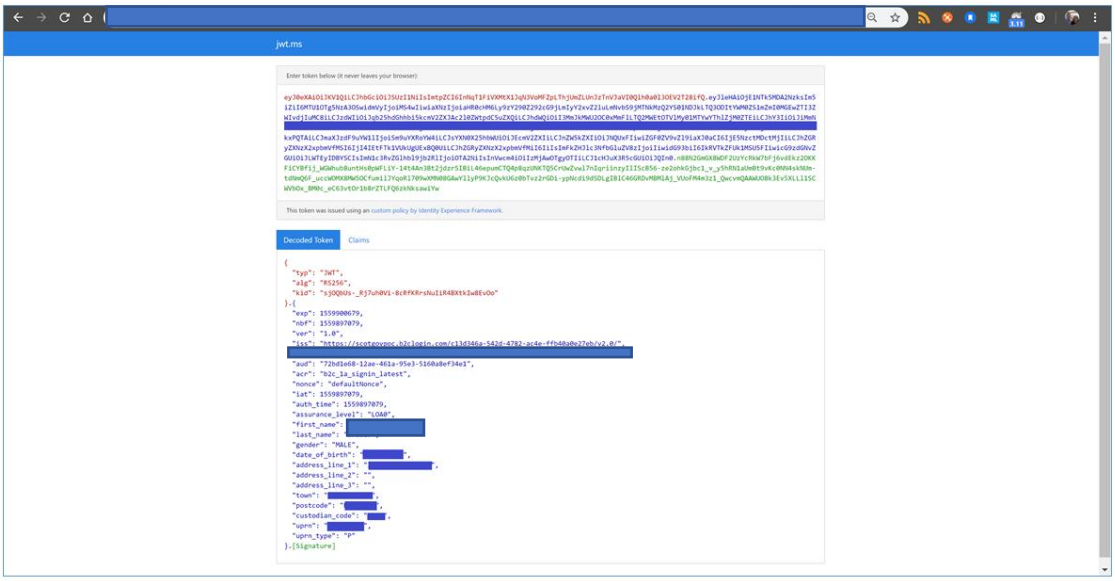

Figure 35 - identity attributes (claims) are returned from myaccount, via digital identity integration layer, for consumption by digital public service

6.3.5 Additional Capabilities

Further to work delivered through this PoC, additional platform capabilities include:

- **Integrating Claims Providers** – Attribute Providers & Attribute Verifiers – this would allow Scottish Government to take advantage of being able to ask their users for permission to gather additional personal data required for the RP's service e.g. a verified National Insurance Number, which could be fulfilled via the DWP service via the Scottish Government Sitekit Identity Assurance Platform.
- **Local accounts** – this would relate to, as an example, the Scottish Government's own IdP associated with Scottish Government branded digital identities and the ability of users to utilise these to assert their identities to Scottish Government and its partners.
- **Social IdP** – this relates to the ability of the user to use existing social media accounts at a lower level of assurance to satisfy the RP's authentication requirement e.g. an LoA0. This feature could also be utilised to hold the attributes associated with the uplift of the user's social ID undertaken within the platform thereby allowing the user to authenticate to the higher level of assurance required by the RP.
- **MFA** – the Multi Factor Authentication capability allows the user to set up a high strength credential within the platform that can be associated with, for example, the user's social ID or with the Scottish Government branded digital identity supported with the platform i.e. the Scottish Government's own IdP.
- **Email verification** – this allows the RP to have more confidence in the email address being presented by the user which in turn ensures that the RP's communications reach the intended recipient and helps reduce the instances where the user needs to initiate the credential recovery process because they set up their email address, also used as their username, incorrectly.
- **User input** – as an example this feature can be used to allow the user to enter and store additional personal attributes and consent to elements of these attributes to be relayed on to the RP. These self-asserted attributes can be converted to verified attributes utilising the platform's links to Attribute Verifiers.
- **User directory** – this would hold the user's identity assurance record associated with, for example, the Scottish Government's own IdP, the uplift of Social IdPs, MFA, additional personal attributes.
- **Token Issuer** – performs a range of functions which includes the transformation and mapping of claims and the support for each RP to use a different protocol such as OIDC or SAML.

7 Next Steps: Beta

Following successful Alpha, Scottish Government should evaluate outcomes and set a clear plan for delivering a live service. This could be a "Beta" programme of work, where end-end functionality is delivered and:

- **Service integration is deliberately limited** (to a small number of candidate digital services – Service A & Service B)
- **In-scope local authorities are deliberately limited** (to a small number of local authorities – Local Authority Y and Local Authority Z – that have bandwidth and resource to support Beta activity)
- **Target user numbers are deliberately small** (to a small number of representative users that have indicated a willingness to trial a demonstration service)
- **In-scope use cases (UCs) are deliberately narrow** (deliver value for the services, local authorities and users in scope and do not aim to "boil the ocean")

Therefore, sample use-cases could include:

- UC1: *As a* ***<Service A User in Local Authority Y>*** *I want* ***<to access Service A using a digital identity I already have / am familiar with>*** *so that* ***<I don't need to set-up and remember another username and password>***
- UC2: *As a* ***<Service B User in Local Authority Y>*** *I want* ***<to access Service B using a digital identity I already have / am familiar with>*** *so that* ***<I don't need to set-up and remember another username and password>***
- UC3: *As a* ***<Service A User in Local Authority Y> >*** *I want* ***<to access Service A using a new digital identity>*** *so that* ***<I can access digital services for the first time>***
- UC4: UC3: *As a* ***<Service B User in Local Authority Y> >*** *I want* ***<to access Service B using a new digital identity>*** *so that* ***<I can access digital services for the first time>***
- UC1: *As a* ***<Service A User in Local Authority Z>*** *I want* ***<to access Service A using a digital identity I already have / am familiar with>*** *so that* ***<I don't need to set-up and remember another username and password>***
- UC2: *As a* ***<Service B User in Local Authority Z>*** *I want* ***<to access Service B using a digital identity I already have / am familiar with>*** *so that* ***<I don't need to set-up and remember another username and password>***
- UC3: *As a* ***<Service A User in Local Authority Z>*** *I want* ***<to access Service A using a new digital identity>*** *so that* ***<I can access digital services for the first time>***
- UC4: UC3: *As a* ***<Service B User in Local Authority Z>*** *I want* ***<to access Service B using a new digital identity>*** *so that* ***<I can access digital services for the first time>***

In addition to general project governance best-practice, Scottish Government should consider:

- Establishing a suitable trust framework that supports:
  - Correct flow of data between system actors
  - Clear liability and payment model
- Appropriate consideration to accessibility, standards compliance, use of device / browser; security assessment; brand, style and tone of voice – ensuring maximal user uptake and use of the system

Appendix A - Glossary

Identity Provider	IdP	An Identity Provider is an entity that creates, maintains, and manages identity information for registered users and provides authentication services to Relying Party applications to allow users to assert their identity to the Relying Party enabling subsequent access to their products & services.
Levels of Assurance	LoA	Levels of Assurance, in the context of identity, relates to the level of confidence that the person presenting the credentials is in fact the real life identity.
	LoA0	This level of assurance provides a low level of confidence as the identity information has been self-asserted by the person and may not even relate to a real life identity.
	LoA2	This level of assurance, as defined within the UK Government Digital Service GPG45, represents a medium level of confidence associated with the degree of identity proofing undertaken and the level of credential utilised by the individual.
Relying Party	RP	In the context of digital identity, a Relying Party is the consumer of the user's identity assertion and associated attributes, leading to the user being able to access the Relying Party's products & services.
Vouching Service		The Vouching Service is a mechanism whereby the Relying Party's representatives or authorised third party representatives can conduct a face to face review of the individual's identity evidence which can be used to increase the level of confidence in an individual's identity and used to uplift their digital identity.

Figure 36 - glossary